Service Level Agreement

This document contains information on all the monitoring and managed services that Remote Monitoring Services (hereby identified as RMS) offers and forms part of the Terms and Conditions of the service. Please refer to the relevant section(s) for the specific service(s) to which you are subscribing (installer) or receive (end user). RMS reserve the right to amend the below without consultation.

GENERIC MONITORING TERMS

ABOUT THIS SERVICE

RMS remotely monitors VSS, Intruder, Panic & Fire systems along with providing other services, such as call handling, environmental, SNMP, virtual concierge services & lone worker monitoring from a National Security Inspectorate (NSI) Regulated Category II Gold Remote Video Receiving Centre (RVRC) and Alarm receiving Centre (ARC) in accordance with BS5979, BS8418, BS9518 and all other relevant standards & regulations for which it is accredited (where applicable) RMS also adheres to ISO9001 for quality management. All monitoring operators are vetted in accordance with BS7858 and licensed by the Security Industry Authority (SIA) for VSS Public Space Surveillance. Remote Monitoring Services monitors multiple sites simultaneously at any given time.

PORTALS & REMOTE ACCESS

RMS provide a range of portals that allow installers and end users connect to our monitoring platform for the viewing of signals, footage, updating details and/or placing systems on test. All portals provide access to sensitive data and can prevent RMS from receiving alarms if the system is placed on test. RMS has implemented standards across its portals that require passwords of a minimum length, as well as time out settings and limits to the how long systems can be placed on test. The standards used comply with British Standards and Cyber Security recommendations.

CONNECTION & SOAK TEST PERIOD

All systems on commencement of monitoring will go through a 14-day soak test period during which time the system is assessed on how it performs, on completion of the soak test period, monitoring commissioning forms will be sent to the installer. During the soak test period calls to the police are prohibited unless visually confirmed criminal activity is observed by the operator. At the end of the initial 14-day soak test if there are outstanding issues which would cause the system to be rejected the soak test would be extended by a further 14-days. At the end of the soak test period, should the system meet the required standard for monitoring the system it will be accepted, if it is not working as expected it will be rejected.

A system will be rejected if any of the following are observed

System Type	Issue Noted
VSS Monitoring	No images received on the alert received
	Alerts received that are a singular image and not video or multiple images
	Images received that are playing backwards
	Excessive alarms that cannot be reduced by using Calipsa or changes to the on-site detection
	Images received that are of a poor quality and impact the operative's ability to identify what is happening on them
	No connection to over 50% of the site
	No connection to a monitored camera where that camera is the only monitored camera on site
	Excessive integrity alarms e.g., video loss, connection monitoring, power loss etc.
	A fully functional camera (PTZ) that is not functioning
	A connection speed on site that impacts the ability to connect to the cameras
	Monitored cameras with their field of views obstructed
	Installations which are not complete
	Poor or no lighting, or poor night-time images that impacts on the operatives ability to identify what is happening on them
Intruder, Hold-Up & Fire Alarm Monitoring	Excessive alarms from zone/s that have not been rectified by the maintainer
	Excessive communication path fails signals
	Communicators in total path fails
	PINs the incorrect way round where the system uses PIN's rather than SIA
	Incorrect protocol for SIA signals
	Signals that have not been tested but are on the connection form

When a system is rejected, it will still be monitored by RMS according to these terms, however RMS do not accept any liability regardless of the reason, should an incident occur on a customers site. Where a system has been rejected it is the client's responsibility to inform RMS once the works have been completed

Operatives will notify by auto generated email any faults observed on the system or with the lighting on site when they are noticed, it is the client's responsibility to arrange for an engineer to attend and rectify the fault. During the soak test period the RMS Technical team will provide updates through the soak test if there are items that require resolution.

Systems can only go live on submission of a monitoring connection form and a site plan (for VSS systems). All new systems, additions and variations of systems need to be tested with RMS prior to them being able to go live.

Failure to provide an RMS monitoring connection form, and a site plan in line with BS9518 requirements for VSS will not go live.

SITE INFORMATION

It is the clients and end users' responsibility to advise RMS of any changes to key holders, telephone numbers, passwords or changes that may affect the monitoring of and response to alarms from a site. All information should be emailed to customerservices@remote-monitoring.co.uk by a member of the site staff listed on the key holder form, or by an employee of the end users maintenance company, or through a key holder update form.

KEYHOLDERS

The NPCC policy states that all premises with Type A Systems shall have at least 2 keyholders. The provision of a Keysafe type device is not an acceptable alternative. Keyholders shall be trained to operate the alarm, be contactable by telephone, have adequate means of transport to attend the premises at all hours, shall have access to all relevant parts of the premises and shall be able to attend within 20 minutes of being notified. Failure to comply with the above instructions could result in the URN being suspended.

If a keyholder is not available for any reason (e.g., sickness, holiday) a replacement must be provided to cover for any keyholder unavailability.

Customers who employ a commercial keyholding company must be aware of the Security Industry Authority (SIA) Licensing Regulations and BS 7984-1 in relation to keyholding and response. NB: If the SIA regulations impede the commercial keyholding company from attending within 20 minutes of being notified, alternative keyholders must be registered to meet compliance with keyholder requirements above.

Failure of keyholders to attend when requested on 2 occasions in a rolling 12-month period will result in the withdrawal of police response for a 3 month period.

Requests for police response should only come from the ARC's. Keyholders should not contact the police asking for their attendance unless they have arrived at the protected premises and there is a crime in progress, or a crime has been committed.

Due to operational demands, responding officers may not always be able to remain at the premises and wait for the keyholder or if there is no obvious sign of a criminal offence.

PASSWORDS & ON TEST PROCESS

RMS employees on receipt of a call from site personnel or their maintainer, will verify the caller through the taking the following information –

1. the code word or the Engineer's code number.
2. The caller's name
3. the name and address of the system

Should the caller fail verification no information relating to the site will be released, nor will any request to place a system on test will be actioned.

When RMS contacts a member of the site staff, they will be asked to confirm their password before any information is released, this is to ensure that the key-holder being contacted is not compromised. Should the duress password is provided the call will be escalated to the local Police Force. Should the member of site staff not have a password listed the alarm information will be passed to them to ensure that the alarm can be investigated, however, the caller can not contact us back and request further information or cancel the alarm. When a key holder update is received, passwords are required to be

provided within the document to ensure that site personnel do have a password and the passing of security information can be done so through a verification process.

The passing of fire alarms does not require a password due to the nature of the alarm.

The passing of alarms to a key holding company does not require a password due to the nature of their business. Key holding companies that are employed to perform a patrol of a site which requires notification to Remote Monitoring Services require a password for verification.

If the caller is requesting that the system be placed on test the Remote Monitoring Services employee will enquire as to how long the testing period will be. The caller should telephone the ARC when testing is complete or if the time for testing needs to be increased.

Any signals received during the test period will be verbally confirmed with the engineer or key-holder (when the account is taken off test) to ensure that the signals showing are correct with the test undertaken.

Any signals received after the test time will be actioned even if it is believed the account is still on test.

SITE ACCESS

The client and end user should ensure all authorised persons on site are informed that they should operate in a way that will minimise the occurrence of spurious activations because of their presence. They should be made aware that entry to the site outside of the normal site opening times should only be made after a call has been made to RMS and they have been verified through the password process, making the operator aware of their intent to enter the site. It is the responsibility of the customer or end user to verify the identity of any persons.

It is not the responsibility of RMS to monitor end user movements on site, monitoring should only take place when the site is vacant, and all employees are off site. Where a site arms up and there are still movements of persons on site RMS will turn the system off until such a time that all persons have left site.

ARMING AND DISARMING

Arming and disarming of remote VSS systems is the responsibility of the end user and should be controlled at the site. RMS employees will only carry out this service for short periods of time with prior agreement with the customer or end user. Where schedules are used in place or a keypad it is the customers responsibility to ensure that these are updated for variations to normal working.

HOUSE KEEPING

The end user must adhere to good housekeeping procedures, such as keeping foliage trimmed and ensuring equipment or vehicles are not blocking camera views or detectors, etc. as well as for keeping lighting in good working order to allow the cameras to operate during the hours of darkness.

RESPONSE TIMES TO ALARM

RMS undertakes to meet the standards for response times to alarms which are as follows –

Alarm Classification	10 Seconds	30 Seconds	40 Seconds	60 Seconds	90 Seconds	180 Seconds
Lone Worker	80%		98.5%			
Fire Alarms		90%		98.5%		
PA/Hold-Up Alarms		80%		98.5%		
Intruder Alarms					80%	98.5%
VSS Alarms					80%	98.5%

CRITICAL DATA OMISSIONS

Where an RMS operative identifies that a listed key holder is no longer at that site the operative will remove the key holder instantly and include this in the report sent at the end of the event, where it is found that a number is incorrect or invalid the operative will include this information within the report sent at the end of the report.

ACCESS TO VSS

Where VSS is installed on a site, Remote Monitoring Services will always have access to this, including when the system is disarmed. This is for remote fault analysis and connection monitoring of the systems.

PRIORITISATION OF ALARM SIGNALS

RMS prioritises alarms from all customers systems in a logical order defined by the risk to the user or end user's business. The prioritisation order is as follows –

Alarm Type	Prioritisation	Notes
Panic Alarm, Hold Up Alarm, Monitored Lone Worker Alarm, Fire Alarm	1	Monitored Lone Worker Alarm is a Missed Check-In or SOS Event
High Priority Infrastructure Critical Monitoring Systems	10	Prioritisation given to alarm types in levels 20,30 & 40 for National Infrastructure Critical Systems
Confirmed Intruder Alarms	20	Signals that are classified as sequential confirmed alarms by the intruder alarm system
VSS Alarm, VSS Camera Tamper Alarm, Intruder System Alarms, Environmental Alarms, Lift Alarms, Sprinkler, Heat & Other Alarms from Fire Systems, Intruder Alarms from VSS Systems	30	Intruder System Alarms Includes, Single Zone Alarms, Tamper, Mains Power Fail. Environmental Alarms Include Freezer, Temperature ETC. VSS Alarms Includes Monitored Access Control Door Alarms
Loss of Connection to VSS Systems & Intruder Communicators, Late to Set, Early to Open, Failed to Set, Other VSS Alarms	40	Other VSS Alarms includes VSS Power Fail Monitoring e.g., UPS, PSU etc. Hard Drive Fails, Video Loss, Intruder Communicators Total Path Comms Loss
Unknown signals	50	Signals Received That Are Defined By The Platform As Unknown/Unprogrammed
Virtual Concierge	60	
Remote Patrols	180	
Helpdesk Services Alarms	190	
Auto Handled Alarms	200-250	Intruder & Fire Communicator Single Path Fails & Signals Where Customers Have Requested To Be Notified Via Email Only

REMOTE VSS & ACCESS MONITORING

A VSS alarm is defined as an alarm that has been triggered from a VSS system by means of an onsite system to detect activity, such alarms would be from analytics, video motion, PIR's, door contacts, trip wires, VSS tampering alarm (with images). VSS system alarms e.g., video loss, hard drive fail, connection monitoring are not VSS alarms.

ACTIONS ON RECEIPT OF A VSS ALARM

On receipt of a VSS alarm activation, the operative will view the images received to identify the cause of the alarm. In the event of the alarm being received from a fully functional camera, the operative will view all pre-set positions or perform a tour of the immediate area to ascertain the cause. If the cause is easily identifiable and presents no threat to the security of the premises, the operative will enter details of their findings in the software provided and close the event.

In the event of the cause of the alarm is not easily identifiable, the operative will view adjacent cameras available to attempt to identify the cause. If there is no visible cause and all attempts have been made to identify the cause of the activation, the operative will enter their findings and actions into the software provided and close connection to site.

Note: for systems that use analytics or video motion, where the detection is done by that camera it is not necessary for the operator to always check the adjoining camera.

When an alarm is received from site and persons are viewed within the perimeter of the premises and verification of attendance has not been received, or whereby the site is classified as open (no hard boundary) or whereby the system always allows access to the public, the operative will view the received and live images to assess the persons actions. On occasions, it will be permissible for the operative to issue an audio (where the functionality is installed), the persons will be warned that

they are being monitored and requesting they leave site immediately. After issuing of an audio warning, if individuals leave site the operative will enter details of the event onto the software provided, in some instances a report will be sent to the customers advising of what has occurred. If deemed necessary, the operative may contact the nominated key holders and request attendance or verification if the operative deems that they are unable to classify the person as no threat.

When an alarm is received, and an intruder can be clearly identified as being within enclosed premises or committing a criminal act, or there is a genuine threat to the property or individuals, the operative will immediately contact the emergency services and key holders and request attendance. The operative will attempt to track and record movements of any suspicious persons seen on images received, with a view to obtaining evidential information for later investigation. All incident reports raised will be emailed to the customer at the earliest opportunity.

In all instances the operative will use their judgement based upon the evidence provided to them within the alarm image, live view and information pertaining the site, e.g., if the site has a solid boundary, the persons demeanour, how the site was gained access to, amongst other considerations.

ACTIONS ON RECEIPT OF A VSS TAMPER

On receipt of a VSS tamper alarm the operative will view the images received to identify the cause. Should the operative observe that the camera has not been tampered with through a change in scenery the event will be closed as a false alert.

Should the operative observe that the camera has moved but there is no criminal activity observed, a fault report will be raised and sent to the customer.

Should the operative observe that the camera has been moved through deliberate tampering the event will be treated as an intruder event, as detailed above for a VSS alarm.

CONNECTION MONITORING & VIDEO LOSS

RMS can on most systems offer a connection monitoring facility, this is a ping sent to a device at intervals of 10 minutes. On three successive fails an alert is generated into the monitoring platform that connection has been lost. Connection monitoring is carried out on NVR's, VMS systems or where the system is decentralised, on the camera directly.
Most NVR's & VMS systems offer the ability for a video loss signal to be sent when it detects that the signal from the camera has been lost. Video loss should be used where available as connection monitoring can not be performed on cameras connected to an NVR or VMS.

The operative will then proceed with actioning this alarm based on the criteria below:

- **Partial Site Loss –** The alert will go through a 30-minute auto suspension period, at the conclusion of this if there is no reconnection an automatic email which will notify the client

- **All Site Loss/Full NVR –** The alert will go through a 30-minute auto suspension period, at the conclusion of this, and there is no reconnection, the operative will contact the key holders by phone and advise them of the loss of connection, an email will also be sent.

GENERIC VSS SYSTEM ALARM

A generic VSS SYSTEM ALARM is defined as an alarm that has been triggered from a VSS system as a notification of a fault e.g., hard drive fail, power loss.

Alarm Type	Action Taken
Power Loss Signals	A call made to the keyholders and an email confirming action taken
Hard Drive Fail etc.	An email sent stating the alarm type has been received

FALSE ALARMS

RMS has a responsibility through the standards it complies with and to all customers to manage false alarms. False alarms are defined as alarms that are not caused by a genuine movement on site of persons.

In the event of multiple and excessive activations (5 activations in 120 minutes) being received, and no visible cause being identified or for a reason determined to be the animal nuisance, foliage, or detection beyond the bounded property, the operative will isolate the offending detection device or camera for a period of 1 hour. If the problem continues, the operative will isolate the offending detector or camera until the problem is rectified. It is the responsibility of the Client to inform the

RVRC that the problem has been rectified and to request reinstatement. Notice will be provided to the client in the form of an auto-generated fault email sent at the time of permanent isolation.

In some instances, where there are excessive alarms from a site but do not trigger the runaway event, permanent isolations may be put in place. Permanent isolations will be notified to the customer via an auto-generated fault e-mail sent at the time of the isolation.

In adverse and unforeseen weather conditions (in particular, where the MET Office has issued a storm warning, but not limited to) the RVRC may isolate cameras that are causing excessive alarms due to environmental conditions for four hours, without a runaway being received. This is to ensure that the number of alarms is decreased, and real alarms of intruders are not hindered by the false alarms.

Whereby a site arms early or disarms late and there is a high amount of activity caused by staff, we will work with the customer to reduce the monitoring times, on occasions for the protection of all customers by controlling alarm activity changes in times will be enforced with the customer notified of these changes.

FILTERING OF ALARMS

Remote Monitoring Services use a Deep Learning Powered Video Monitoring solution from a trusted partner, Calipsa for the filtering of VSS alarms triggered by video motion, video analytics or other similar systems, whereby the camera is defined as static.

Alarms are triggered from the end user's system and sent either to Remote Monitoring Services systems first and then are passed to Calipsa or are delivered direct to Calipsa. At Calipsa the deep learning system analyses the images for movement of a person and or a vehicle, if such movement is detected the alert is passed to a Remote Monitoring Services employees for further analysis. If no such movement is detected the alarm is flagged as false and is not presented to a Remote Monitoring Services employees for analysis.

Where a VSS and an intruder alarm system are monitored together for a site, RMS will filter out VSS alarms from a site that are received within 2 minutes of an arm signal being received as the default setting. This is then assessed on a case-by-case basis and can be increased should it take longer for end users to vacate the site.

Video Loss, connection loss monitoring, VSS power loss monitoring are all subject to a 30-minute filtering policy. Filtering is applied immediately on receipt of the alarm from the transmission device. Should the same device and or transmission unit send a restore that compliments the failure signal the alert is automatically closed by the system with no notification made. If at the end of the filtering period, no restore alert has been received the signal is presented to an operative to respond to.

PROCEDURE FOR NOTIFYING KEY HOLDERS

RMS adheres to the following procedure when contacting key holders –

- **Initial Calling of a Key holder** – The ARC will allow the Key Holder's telephone to ring for a reasonable amount of time for the call to be answered. If there is no answer after a reasonable amount of time an attempt will be made to contact the next listed Key Holder.

- **The Key Holders Telephone is Engaged** – An engaged telephone number will only be re-tried on the next round of calls if another key holder cannot be contacted in the meantime.

- **Key holders on Answer Phones –** The ARC will not, on the first attempt to contact a key holder, leave a message on an answerphone. However, if on a further attempt, a Key Holder is still on answerphone, a short message will be left requesting the Key Holder telephones the ARC.

- **Leaving Messages if Key holder is unavailable –** The ARC will not leave messages with any person who appears to be under 16 (sixteen) years of age. Where messages have been left, it will not affect the continued attempts by the ARC to contact a Key Holder.

- **Continued Attempts to Contact a Keyholder –** Where on the first round of calls a keyholder is not spoken to RMS will attempt to contact each keyholder at least 20 (twenty) minutes after the initial call. If on this second round of calls a keyholder does not answer a message will be left where an answerphone service is available. Once all listed keyholders have been attempted the call will be classified as closed.

- **Key holders unable to attend –** If a key holder is unable to attend, or chooses not to attend, the ARC will not continue with attempts to contact any other key holder. It will be deemed that the activation has become the responsibility of the customer and will be regarded by us as closed.

RMS cannot enter any commitment which would involve assuming the powers of civil Police.

LATE TO SET

If requested by the customer, within a predetermined set of minutes, as advised by the customer, of the latest arming times, the operative will identify if the system has been armed. If the system has not been armed, the operative will contact the nominated emergency Key Holder contact to enquire as to the delay in the arming times. The operative will then raise an incident report which will be emailed to the client at the earliest opportunity. To be able to perform a late-to-set check, the ARC must be able to receive a separate armed and disarmed signal from the system.

EARLY TO OPEN

In the event of the remote VSS System becoming disarmed before the appropriate time, the operative will contact the key holder contact to verify attendance at the premises. The operative will then raise an incident report which will be emailed to the customer at the earliest opportunity. To be able to perform an early-to-open check, the ARC must be able to receive a separate armed and disarmed signal from the system.

STORAGE OF IMAGES

RMS only stores images from alarms received and from the live view investigation of the alarm. These images are kept for 30 days. Where there is an incident on site Remote Monitoring Services will store the footage of what the operative has observed for 365 days for evidential purposes, after this point it will be deleted.

INTRUDER ALARM MONITORING

ACTIONS ON RECEIPT OF ACTIVATIONS

RMS's response will change on the business day following the successful completion of the soak test period, to the following, unless the end user or the maintainer, advises the ARC to extend the test period.

Alarm Type	Action	Further Notes
Confirmed Intruder Alarm (URN)	Police then keyholders	Email report on completion of actions
Confirmed Intruder Alarm	Keyholders	Email report on completion of actions
Intruder Alarm	Keyholders	Email report on completion of actions
Intruder Integrity Alarms e.g. Mains Power, Tamper Alarms	Keyholders	Email report on completion of actions
Late to Close, Early to Close, Fail to Set	Keyholders	Email report on completion of actions
Battery Fails, Battery Low, Data Loss, Weak Signals, Network Fault, RF Interface, Battery Trouble, Low Voltage	Auto Generated Email	
Communication Path Failure With At Least One Path Remaining Live	Auto Generated Email	
Path Failure With No Paths Remaining Live	Keyholders	Email report on completion of actions

POLICE RESPONSE

RMS can only notify the Police on receipt of a confirmed intruder alarm from the system if a valid URN is supplied. If no URN is supplied, then confirmed alarms will be passed to a Key Holder in the same respect of an unconfirmed or other alarm type. The exception to this rule is if there is VSS that RMS has access to and when checked, the operative can verify criminal activity taking place, should the operative not be able to verify criminal activity the Police cannot be contacted.

As the maintainer owns the URN a fee will not be charged to the customer for every false alarm passed to the Emergency Services. However, after the specified number of false alarms the URN will be withdrawn by the emergency services.

It is the responsibility of the maintainer to inform RMS if a URN is withdrawn by the emergency services, and to undertake the necessary actions to regain the URN. It is also the responsibility of the maintainer to inform the end user of the status of Police response.

NOTE: Withdrawal of a URN can invalidate the end user's insurance policy.

FILTERING POLICY

RMS understands the importance of reducing the number of false alarm calls passed to the Police and has put the following procedures in force to filter Intruder Alarm Signals in accordance with the National Police Chiefs Council (NPCC) Policy and NSI Code of Practice.

All systems shall either:

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

RMS will filter single, confirmed intruder signals, tamper & general faults for a maximum of 120 seconds to allow the alarm to be aborted or to await the secondary confirmed alarm.

Single path fails are filtered for a 30-minute window automatically by the monitoring platform on receipt of the alert. If a restore for the same transmission unit is received during this window the alarm is closed and not presented to an operative to action. If at the end of the window a restore has not been received, then the system handles the alert and sends an auto-generated email to notify of the path being in the loss state.

Full path fails are filtered for a 30-minute window automatically by the monitoring platform on receipt of the alert. If a restore for the same transmission unit is received during this window the alarm is closed and not presented to an operative to action. If at the end of the window a restore has not been received, then the alarm is presented to an operative for handling who will contact a key holder.

Mains power fail alarms are filtered for a 30-minute window automatically by the monitoring platform on receipt of the alert. If a restore for the same transmission unit is received during this window the alarm is closed and not presented to an operative to action. If at the end of the window a restore has not been received, then the alarm is presented to an operative for handling who will contact a key holder.

During adverse and unforeseen circumstances, it is permissible for RMS to extend the filtering delay until such a time that the circumstance has passed. During these extended filtering times signals may be closed by the system automatically should an open signal or restore signal be received during the time.

EXCESSIVE FALSE ALARMS

RMS may isolate alarms from an alarm system in the event of multiple and excessive activations (5 activations in 120 minutes) being received, the operative will isolate the offending alarm for a period of 1 hour. If the problem continues, the operative will isolate the offending alarm for a further 1 hour.

Should during a conversation with the keyholder they confirm that the alarm should be isolated for longer, then the operative will isolate for the agreed length of time.

Notice will be provided to the client in the form of an auto-generated email sent at the time of the isolation.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the maintenance engineer or in some cases the end user to place systems on and off test with the ARC.

PROCEDURE FOR NOTIFYING KEY HOLDERS

RMS adheres to the following procedure when contacting key holders –

- **Initial Calling of a Key holder** – The ARC will allow the Key Holder's telephone to ring for a reasonable amount of time for the call to be answered. If there is no answer after a reasonable amount of time an attempt will be made to contact the next listed Key Holder.

- **The Key Holders Telephone is Engaged** – An engaged telephone number will only be re-tried on the next round of calls if another key holder cannot be contacted in the meantime.

- **Key holders on Answer Phones –** The ARC will not, on the first attempt to contact a key holder, leave a message on an answerphone. However, if on a further attempt, a Key Holder is still on answerphone, a short message will be left requesting the Key Holder telephones the ARC.

- **Leaving Messages if Key holder is unavailable –** The ARC will not leave messages with any person who appears to be under 16 (sixteen) years of age. Where messages have been left, it will not affect the continued attempts by the ARC to contact a Key Holder.

- **Continued Attempts to Contact a Keyholder –** Where on the first round of calls a keyholder is not spoken to RMS will attempt to contact each keyholder at least 20 (twenty) minutes after the initial call. If on this second round of calls a keyholder does not answer a message will be left where an answerphone service is available. Once all listed keyholders have been attempted the call will be classified as closed.

- **Key holders unable to attend –** If a key holder is unable to attend, or chooses not to attend, the ARC will not continue with attempts to contact any other key holder. It will be deemed that the activation has become the responsibility of the customer and will be regarded by us as closed.

LATE TO SET

If requested by the customer, within a time window as supplied by the customer, of the latest arming times, the operative will identify if the system has been armed. If the system has not been armed, the operative will contact the nominated emergency key holder contact to enquire as to the delay in the arming times. The operative will then raise an incident report which will be emailed to the customer at the earliest opportunity. To be able to perform a late-to-set check, the ARC must be able to receive a separate armed and disarmed signal from the system.

EARLY TO OPEN

In the event of the intruder system becoming disarmed before the appropriate time, the operative will contact the nominated key holder to verify attendance at the premises. The operative will then raise an incident report which will be emailed to the Client at the earliest opportunity. To be able to perform an early-to-open check, the ARC must be able to receive a separate armed and disarmed signal from the system.

FIRE ALARM MONITORING

ACTIONS ON RECEIPT OF AN ALARM

RMS's response will change on the business day following the successful completion of the soak test period, to the following, unless the customer or the maintainer, advises the ARC to extend the test period.

Alarm Type	Action	Further Notes
Fire Alarm (System Disarmed)	Keyholders	Email report on completion of actions
Fire Alarm (System Armed)	Fire Brigade then keyholders	Email report on completion of actions
Other Fire Related Signals – Sprinkler Alarms, Heat Alarms	Keyholders	Email report on completion of actions
Fire Fault	Keyholders	Email report on completion of actions
Communication Path Failure With At Least One Path Remaining Live	Auto Generated Email	
Path Failure With No Paths Remaining Live	Keyholders	Email report on completion of actions

FIRE BRIGADE RESPONSE

Most Fire Brigades will no longer respond to fire alarms from commercial properties whilst there are employees on site. Domestic properties and properties where there are residents sleeping are generally exempt from this.
For commercial properties, RMS will only notify the Fire Brigade on receipt of a fire alarm from the system when the site is closed, when there are employees on site it is the end user's responsibility to contact the Fire Brigade if there is a fire.
Note that Fire Scotland no longer respond to fire alarm signals unless verified via technology identifying a confirmed fire or by visual confirmation from a keyholder, inclusive on when the sites intruder system identifies the site as armed. For all systems in Scotland where the fire system is remotely monitored, unless confirmatory technology is installed and signals to Remote Monitoring Services, the alarm will be passed to key holders only and it is the keyholders responsibility to contact the fire brigade if there are signs of fire.

FILTERING POLICY

No filtering policy is applied to fire alarm signals unless a specific request is made by the customer's local brigade.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the maintenance engineer or in some cases the end user to place systems on and off test with the ARC.

PROCEDURE FOR NOTIFYING KEY HOLDERS

RMS adheres to the following procedure when contacting key holders -

- **Initial Calling of a Key holder** - The ARC will allow the Key Holder's telephone to ring for a reasonable amount of time for the call to be answered. If there is no answer after a reasonable amount of time an attempt will be made to contact the next listed Key Holder.

- **The Key Holders Telephone is Engaged -** An engaged telephone number will only be re-tried on the next round of calls if another key holder cannot be contacted in the meantime.

- **Key holders on Answer Phones -** The ARC will not, on the first attempt to contact a key holder, leave a message on an answerphone. However, if on a further attempt, a Key Holder is still on answerphone, a short message will be left requesting the Key Holder telephones the ARC.

- **Leaving Messages if Key holder is unavailable -** The ARC will not leave messages with any person who appears to be under 16 (sixteen) years of age. Where messages have been left, it will not affect the continued attempts by the ARC to contact a Key Holder.

- **Continued Attempts to Contact a Key holder -** Where on the first round of calls a keyholder is not spoken to RMS will attempt to contact each keyholder at least 20 (twenty) minutes after the initial call. If on this second round of calls a keyholder does not answer a message will be left where an answerphone service is available. Once all listed keyholders have been attempted the call will be classified as closed.

- **Key holders unable to attend -** If a key holder is unable to attend, or chooses not to attend, the ARC will not continue with attempts to contact any other key holder. It will be deemed that the activation has become the responsibility of the customer and will be regarded by us as closed.

HOLD-UP ALARM MONITORING

ACTIONS ON RECEIPT OF ACTIVATIONS

RMS's response will change on the business day following the successful completion of the soak test period, to the following, unless the customer or the maintainer, advises the ARC to extend the test period.

Alarm Type	Action	Further Notes
Hold Up Alarm (URN)	Keyholders & Police	Email report on completion of actions
Hold Up Alarm (No URN)	Keyholders*see Police Response below	Email report on completion of actions
Hold Up Alarm (Visual Confirmation)	Keyholders & Police	Email report on completion of actions
Fault signals	Keyholders	Email report on completion of actions

POLICE RESPONSE

RMS will only notify the Police on receipt of a Hold-Up alarm from the system if a valid URN is supplied or if there is visual or visual technology accompanying the alarm. If no URN or conformational technology is supplied, then Hold-Up alarms will be passed to a key-holder in the same respect of another alarm type. Should the user/location of the HUA be a keyholder then RMS will on receipt of confirmation from the user that Police are required contact the Police.

As the maintainer owns the URN a fee will not be charged to the customer for every false alarm passed to the Emergency Services. However, after the specified number of false alarms the URN will be withdrawn by the emergency services.

It is the responsibility of the maintainer to inform RMS if a URN is withdrawn by the emergency services, and to undertake the necessary actions to regain the URN. It is also the responsibility of the maintainer to inform the end user of the status of Police response.

NOTE: Withdrawal of a URN can invalidate the end user's insurance policy.

FILTERING POLICY

No filtering is applied to hold up alarms.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the maintenance engineer or in some cases the end user to place systems on and off test with the ARC.

PROCEDURE FOR NOTIFYING KEY HOLDERS

RMS adheres to the following procedure when contacting key holders -

- **Initial Calling of a Key holder** - The ARC will allow the Key Holder's telephone to ring for a reasonable amount of time for the call to be answered. If there is no answer after a reasonable amount of time an attempt will be made to contact the next listed Key Holder.

- **The Key Holders Telephone is Engaged -** An engaged telephone number will only be re-tried on the next round of calls if another key holder cannot be contacted in the meantime.

- **Key holders on Answer Phones -** The ARC will not, on the first attempt to contact a key holder, leave a message on an answerphone. However, if on a further attempt, a Key Holder is still on answerphone, a short message will be left requesting the Key Holder telephones the ARC.

- **Leaving Messages if Key holder is unavailable -** The ARC will not leave messages with any person who appears to be under 16 (sixteen) years of age. Where messages have been left, it will not affect the continued attempts by the ARC to contact a Key Holder.

- **Continued Attempts to Contact a Key holder -** Where on the first round of calls a keyholder is not spoken to RMS will attempt to contact each keyholder at least 20 (twenty) minutes after the initial call. If on this second round of calls a keyholder does not answer a message will be left where an answerphone service is available. Once all listed keyholders have been attempted the call will be classified as closed.

- **Key holders unable to attend -** If a key holder is unable to attend, or chooses not to attend, the ARC will not continue with attempts to contact any other key holder. It will be deemed that the activation has become the responsibility of the customer and will be regarded by us as closed.

VIRTUAL CONCIERGE

ACTIONS ON RECEIPT OF ACTIVATIONS

On receipt of an activation and call through to the RVRC, the operative will view the images received, the operative will follow a pre-defined script which will involve asking the caller for their name, company name and password to gain access to the site; once the operator has established that the caller is allowed access this will be granted.

If the caller is not listed as permitted access or cannot provide a correct password, then the operator will decline access. It is the caller's responsibility to contact the appropriate site person to acquire the rights to gain access to the premises. The operative will input all information into the monitoring software and close the event with an outcome that will produce an auto-generated email to the customer.

LOSS OF CONNECTION

On a loss of connection to the site, RMS will be unable to provide access to the site unless a secondary communication path has been installed. If a secondary path has not been installed RMS will notify the customer on loss of connection. It is the customer's responsibility to provide access to the site in these instances.

FILTERING POLICY

No filtering is applied to this service.

PATROLS

Actions to be taken on a patrol will be governed by the customers requirement for these. Patrols do not have a response time and the time requested that these occur may not be the time that these take place as alarm response requirements take priority.

ENVIRONMENTAL, SERVER HOSTING & SNMP MONITORING

Actions on alarms will be to contact a keyholder and send a report notification at the conclusion of handling the event. Should the end user require further actions to be taken this should be detailed in the relevant section within the connection form.

GUARDIAN LONE WORKER

RMS provides a lone Worker solution powered by Corrin Guardian Lone Worker Solution; this solution is not BS8484 accredited.

ACTIONS ON RECEIPT OF ACTIVATIONS

On receipt of an activation to the RVRC/ARC the operative will follow our default action plan for signals received as detailed below, unless the customer has provided a variation to these –

- **Start Session –** auto handled by the monitoring platform
- **End Session –** auto handled by the monitoring platform
- **Missed Check-In –** escalated to key holders
- **SOS Event –** escalated to key holders
- **SOS Resolved –** auto handled by the monitoring platform

PINGING A USER FOR LOCATION

Through the Guardian portal, RMS or an admin, can ping the current location of a user. Safety features have been built into the system that restricts the use of the ping function to when users are in an active session only, outside of being in an active session the ability to ping the user isn't available. This function is built into the platform to establish the users current location which may have changed since they started the session. Pinging a user should only be used in the following instances

- When they have missed a check-in
- Triggered an SOS

Whilst a user is in either of these two instances pinging may be carried out by an ARC operative on regular occasions, if required, to provide the information to key holders, until the user is safe.

EMERGENCY SERVICES RESPONSE

RMS cannot contact the emergency services for this service

FILTERING POLICY

No filtering policy is applied to any signals from Corrin Guardian Lone Worker.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the maintenance engineer or in some cases the end user to place systems on and off test with the ARC.

PROCEDURE FOR NOTIFYING KEY HOLDERS

RMS adheres to the following procedure when contacting key holders -

- **Initial Calling of a Key holder** - The ARC will allow the Key Holder's telephone to ring for a reasonable amount of time for the call to be answered. If there is no answer after a reasonable amount of time an attempt will be made to contact the next listed Key Holder.

- **The Key Holders Telephone is Engaged -** An engaged telephone number will only be re-tried on the next round of calls if another key holder cannot be contacted in the meantime.

- **Key holders on Answer Phones -** The ARC will not, on the first attempt to contact a key holder, leave a message on an answerphone. However, if on a further attempt, a Key Holder is still on answerphone, a short message will be left requesting the Key Holder telephones the ARC.

- **Leaving Messages if Key holder is unavailable -** The ARC will not leave messages with any person who appears to be under 16 (sixteen) years of age. Where messages have been left, it will not affect the continued attempts by the ARC to contact a Key Holder.

- **Continued Attempts to Contact a Key holder -** Where on the first round of calls a keyholder is not spoken to RMS will attempt to contact each keyholder at least 20 (twenty) minutes after the initial call. If on this second round of calls a keyholder does not answer a message will be left where an answerphone service is available. Once all listed keyholders have been attempted the call will be classified as closed.

- **Key holders unable to attend -** If a key holder is unable to attend, or chooses not to attend, the ARC will not continue with attempts to contact any other key holder. It will be deemed that the activation has become the responsibility of the customer and will be regarded by us as closed.

HELPDESK SERVICES

CONTRACTED HOURS OF SERVICE

The service is to be provided during the hours of 1700 – 0800 Monday – Friday and all day on weekends, as well as on bank holidays as defined by the government https://www.gov.uk/bank-holidays at all other hours the service may incur additional charges.

CALL WAITING TIME

No minimum nor maximum time for calls to be answered is provided with the service

CALL SERVICE

Calls are to be diverted from the customer's number to a number provided by RMS. The calls will be answered in the name of the customer on the basis that the calls are identified as originating from the customer, at all other times, where the originator is not known, the call is answered in the supplier's name.

The information to be taken from the caller will be detailed by the subscriber, if no information is provided default information of, callers name, number, reason for phone call and site name will be taken.

ALARM RESPONSE SERVICE - RSPNDR

RMS provides to subscribing users an alarm response service, which is delivered by RSPNDR (https://RSPNDR.io), RMS in this instance is a reseller of the service. The service is a monthly subscription which includes 2 call outs within the subscription fee, additional charges are payable for callout exceeding 2 in a 12-month period as well grounding fees (where a guard remains on site awaiting a key holder attending).

SERVICE

On receipt of an intruder alarm signal (single or confirmed) and the site being closed, RMS will request a security officer attends through RSPNDR. The attending officer will conduct an external inspection of the property to try and establish the cause of the alarm event; in particular, look for signs of intruders or damage and report the findings to the alarm monitoring station. This report will be supported by photographic evidence of the inspection and findings.

Should the officer's investigation find that there has been a break-in the officer will advise a site key holder and request attendance the guard will either remain on site until the site personnel attend or if instructed to do so by the site personnel leave site, the attending key holder is to contact the Police on arrival at site and confirmation made of the break-in.

GUARD COMPANY STANDARDS

RSPNDR contracts guard providers to ensure that:

- Each Guard, at all times during its provision of services, will:
  - be in full uniform.
  - have a badge/identification which clearly indicates them to be a guard.
  - drive a vehicle marked with the name and logo of the company that the guard is employed by.
  - be a fully licensed and professionally accredited.
  - perform the guard response services in a safe manner.
  - consistently present a professional image in personal and professional demeanour, communications, and actions in all contacts with RMS's customers and the general public.

Upon arriving at a site, in each instance, the guard shall:

- respond to software prompts to confirm that the guard has arrived on site.

- conduct a complete exterior patrol and inspection of the Site, including any outdoor storage areas, compounds, and garages; inspect any vehicles on site; question and identify any unauthorized people on site; check for evidence of trespass or vandalism at all entrance ways and windows at the site.
- if applicable, conduct an interior inspection of the site.
- while patrolling and inspecting the site, the guard shall complete an incident summary through use of the RSPNDR App and submit such incident summary to the SaaS software, and will use discretion to determine the site status.
- if required, will communicate, and contact the appropriate authority (e.g., police or monitoring station) through the SaaS software
- in case of actual or suspended break-ins to the site, notify the police immediately of such break-in and then immediately notify monitoring station of the same, and then remain on site for further direction from client.
- only remain at the Site and engage in standby/grounding procedures if a standby/grounding request is approved by client, and if the standby/grounding request is so approved will remain at site for standby/grounding procedures until released by client.

Each guard provider holds appropriate professional certification and insurance cover.