Monitoring Terms

The below contains information on all the monitoring and managed services we offer and forms part of the Terms and Conditions of the service available at https://www.businesswatchgroup.co.uk/terms-conditions/. Please refer to the relevant section(s) for the specific service(s) to which you are subscribing. BusinessWatch Group reserve the right to amend the below without consultation.

Generic Remote Monitoring Terms and Agreement

ABOUT THIS SERVICE

BusinessWatch Group remotely monitors CCTV, Intruder, Panic & Fire systems along with providing other services, such as call handling environmental, SNMP & virtual concierge services 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 and all other relevant standards & regulations for which it is accredited (where applicable). All monitoring operators are vetted in accordance with BS7858 and licensed by the Security Industry Authority (SIA) for CCTV Public Space Surveillance. BusinessWatch Group monitors multiple sites simultaneously at any given time

SOAK TEST PERIOD

All systems on commencement of monitoring will go through a 14-day soak test period, on completion of the soak test period, monitoring commissioning forms will be sent to the customer and full monitoring will commence. During the soak test period calls to the police are prohibited unless visually confirmed criminal activity is observed by the operator. Should the system not meet the required standard for monitoring, there are faults observed or the site do not use the system correctly then the soak test period will be extended by a further 7-day period, at the end of this, the system will either by accepted if it is working as expected or rejected if not.

The operator 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.

PLACING SYSTEMS ON TEST

When an operator takes a telephone request for a system to be placed on test the identity of the caller must be confirmed even if the ARC Operative knows the caller, the following will need to be confirmed before an account is placed on test:

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

ARC operatives will ask for and check all Engineers' identity codes are correct. If any of the details given are false or incorrect the account will not be put on test even if the Alarm Receiving Centre Operator knows the caller.

The caller placing the system on test must notify the operator 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 must be verbally confirmed with the Engineer/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 INFORMATION

It is the Client's responsibility to advise BusinessWatch Group 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

SERVICE LEVEL AGREEMENT

PASSWORDS
BusinessWatch Group operators will only speak to site personnel, in relation to the security of the system and alarm events, who are listed on the staff list and who have a valid password. When BusinessWatch Group 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. Failing to provide a valid password will result in the operator escalating the call to another key-holder, if the duress password is provided the call will be escalated to the local Police Force.

SITE ACCESS
With regards to British Standard 8418 Section 7.3, the Client should ensure all authorised persons on site are informed that they should operate in a way that will minimise the occurrence of spurious activations as a result 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 the RVRC, making the operator aware of their intent to enter the site. It is the responsibility of the Client to verify the identity of any persons.

ARMING AND DISARMING
Arming and disarming of remote CCTV systems is the responsibility of the Client. RVRC personnel will only carry out this service for short periods of time with prior agreement with the Client. It is the Client's responsibility to ensure that the RVRC is made aware of Bank Holiday opening and closing times to ensure that monitoring is carried out when required.

HOUSE KEEPING
The Client must test the system on a regular basis. The Client must adhere to good housekeeping procedures, such as keeping foliage trimmed and ensuring equipment or vehicles are not blocking camera views or detectors, etc. The client is responsible for checking that all recorders are recording. Client is responsible for keeping lighting in good working order to allow the cameras to operate during the hours of darkness. If the Client requires regular integrity tests to be carried out, this requirement must be agreed in writing and detailed in this document. Tests will be carried out Monday to Friday between 0900-1600 hours.

RESPONSE TIMES TO ALARMS
In normal circumstances BusinessWatch Group undertakes to meet the standards for contacting the emergency services as set out in BS5979:2007 for Category II ARC's & RVRC's, which are:

1. For PA alarms (where the first action is to the Police): 30 seconds for 80% of signals received and 60 seconds for 98.5% of signals received.

2. For fire alarms (where the first action is to the Fire Authority): 30 seconds for 90% of signals received and 60 seconds for 98.5% of signals received.

3. For intruder alarms (where the first action is to the Police Authority): 90 seconds for 80% of signals received and 180 seconds for 98.5% of signals received exclusive of any alarm filtering period as required by BS5979: 2007

4. For CCTV alarms: 90 seconds for 80% of signals received and 180 seconds for 98.5% of signals received

ACCESS TO CCTV
Where CCTV is installed on a site, BusinessWatch Group will always have access to this, including when the system is disarmed. This is for remote fault analysis and connection monitoring of the systems.

Calipsa Video Monitoring Service
BusinessWatch Group use a Deep Learning Powered Video Monitoring solution from a company called Calipsa. The service analyses alarms received from customer's sites for people and vehicles moving. Positive reads are then notified to for analysis by an operator who will respond in the appropriate fashion

REMOTE CCTV & ACCESS MONITORING

ACTIONS ON RECEIPT OF ACTIVATIONS

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

In the event of the cause of the activation is not easily identifiable, the RVRC Operator 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 RVRC Operator 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.

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 RVRC Operator will isolate the offending detection device or camera for a period of 1 hour. If the problem continues, the RVRC Operator 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 customer 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. These will be notified to the customer via an auto-generated fault e-mail sent at the time of the isolation.

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.

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.

In the event of an activation 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 RVRC Operator 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 issue of audio warning, if individuals leave site the RVRC Operator 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. In the event of persons not leaving site as requested or if deemed necessary, the RVRC Operator will contact the nominated key holders and request attendance. In the event of an activation 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 RVRC operative will immediately contact the emergency services and key holders and request attendance. The RVRC 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.

PROCEDURE FOR NOTIFYING KEY HOLDERS

BusinessWatch Group will try each key holder twice when there is an ongoing incident, after the second attempt to all key holders no further attempt will be made.

BusinessWatch Group cannot enter into any commitment which would involve assuming the powers of civil Police.

CONNECTION MONITORING AND FAULT REPORTING

BusinessWatch Group 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 made to the Operators that connection has been lost. The Operators will then proceed with actioning this alarm based on the table below:

Partial Site Connection 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 customer

All Site Connection Loss

The alert will go through a 30-minute auto suspension period, at the conclusion of this if there is no reconnection contact the key holders by phone and advise them of the loss of connection then use the relevant outcome which will generate an automatic email which will notify the customer

All other faults are reported to the customer via automated email as and when they are notified to the operator through a signal from the site or in the case of lighting when the operator notes the fault.

STORAGE OF IMAGES

BusinessWatch Group 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 BusinessWatch Group will store the footage of what the operator has observed for 365 days for evidential purposes, after this point it will be deleted.

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 RVRC operative will identify if the system has been armed. If the system has not been armed, the RVRC operative will contact the nominated emergency Key Holder contact to enquire as to the delay in the arming times. The RVRC 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 CCTV System becoming disarmed before the appropriate time, the RVRC operative will contact the nominated emergency Key Holder contact to verify attendance at the premises. The RVRC 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.

INTRUDER ALARM MONITORING

ACTIONS ON RECEIPT OF ACTIVATIONS

The BusinessWatch Group 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.

Confirmed Intruder Alarm - Key holder Contacts (and Police if a URN is supplied)
Unconfirmed Intruder Alarm - Key holder Contacts
Intruder Alarm followed by an Open or Abort, within the Filtering Period - No Action Required
All other alarm types (except single path fails) Key holder Contacts
Single path fails - email notification only

POLICE RESPONSE

BusinessWatch Group will 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. As the customer/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 customer/maintainer to inform BusinessWatch Group if a URN is withdrawn by the emergency services, and to undertake the necessary actions to regain the URN.

NOTE: At all times it will be the responsibility of the maintainer to advise the end user (and vice versa) of the current status of Police response and the responsibility of the maintainer/end user to inform the ARC. In the event of more than one Police alarm signal is received at the same time, only the highest priority alarm will be actioned.

FILTERING POLICY

BusinessWatch Group 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 Association of Chief Police Officers' (ACPO) 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". BusinessWatch Group will filter the first signal for a minimum of 120 seconds to allow the alarm to be aborted or to await the secondary confirmed alarm. Path fails are filtered for a longer time period, to allow for a restore.

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. All signals received at the ARC, unless on test, will result in the signal being actioned in the normal way. On discovering that a signal has been transmitted whilst the system was being tested, without notification to the ARC, the customer will be informed via auto generated incident email.

PROCEDURE FOR NOTIFYING KEY HOLDERS

Initial Ringing 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 reply 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 if all other key holders cannot be contacted.

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:
The ARC will continue attempting to contact each key holder at 20 (twenty) minute intervals. No further attempts will be made to contact a key holder where a message has been left on his/her answerphone. In respect of key holders who do not have voicemail, the ARC will continue to try and make contact for 180 (one hundred and eighty) minutes.

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. Should the site be open BusinessWatch Group will contact the site number in the first instance.

CONNECTION LOSS SIGNALS
BusinessWatch Group will only report by telephone call a total communications loss on the system. Should a connection loss be received by one of the 2 lines of communication this will be notified via email.

Recurrent and/or intermittent connection signals will be placed on test until such a time that the customer resolves the issue.

LATE TO SET
If requested by the customer, within a time window as supplied by the customer, of the latest arming times, the ARC operative will identify if the system has been armed. If the system has not been armed, the ARC operative will contact the nominated emergency key holder contact to enquire as to the delay in the arming times. The RVRC 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 remote CCTV System becoming disarmed before the appropriate time, the ARC operative will contact the nominated emergency Key Holder contact to verify attendance at the premises. The ARC 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.

FIRE ALARM MONITORING

ACTIONS ON RECEIPT OF AN ALARM

The BusinessWatch Group 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.

Fire Alarm when site is closed - Fire Brigade then Key holder Contacts
Fire Alarm when site is open - Key holder Contacts
All other alarm types (except single path fails) Key holder Contacts
Single path fails - email notification only

FIRE BRIGADE RESPONSE
BusinessWatch Group will only notify the Fire Brigade on receipt of a fire alarm from the system when the site is closed. Fire Brigades will not respond to a fire alarm if a site is open when staff is on site, it is the Client's responsibility to contact the Fire Brigade during opening hours.

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. All signals received at the ARC, unless on test, will result in the signal being actioned in the normal way. On discovering that a signal has been transmitted whilst the system was being tested, without notification to the ARC, the customer will be informed via auto generated incident email.

PROCEDURE FOR NOTIFYING KEY HOLDERS
Initial Ringing 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 reply 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 if all other key holders cannot be contacted.
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:
The ARC will continue attempting to contact each key holder at 20 (twenty) minute intervals. No further attempts will be made to contact a key holder where a message has been left on his/her answerphone. In respect of key holders who do not have voicemail, the ARC will continue to try and make contact for 180 (one hundred and eighty) minutes.

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. Should the site be open BusinessWatch Group will contact the site number in the first instance.

CONNECTION LOSS SIGNALS
BusinessWatch Group will only report by telephone call a total communications loss on the system. Should a connection loss be received by one of the 2 lines of communication this will be notified via email.
Recurrent and/or intermittent connection signals will be placed on test until such a time that the customer resolves the issue

HOLD-UP ALARM MONITORING

ACTIONS ON RECEIPT OF ACTIVATIONS
The BusinessWatch Group 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.

Panic Alarm (URN) - Key holder Contacts (and Police if a URN is supplied)
Panic Alarm (no URN) - Key holder Contacts
Panic Alarm (with visual or sound confirmation) -Key holder Contacts and Police
All other alarm types - Key holder Contacts

POLICE RESPONSE
BusinessWatch Group will only notify the Police on receipt of a Panic 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 panic alarms will be passed to a key-holder in the same respect of another alarm type.

As the Customer/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 Customer/Maintainer to inform BusinessWatch Group if a URN is withdrawn by the Emergency Services, and to undertake the necessary actions to regain the URN.

NOTE: At all times it will be the responsibility of the installer to advise the End User (and vice versa) of the current status of Police response and the responsibility of the Installer/End User to inform the ARC. In the event of more than one policed alarm signal is received at the same time, only the highest priority alarm will be actioned.

FILTERING POLICY
No filtering policy is applied to panic alarm signals.

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. All signals received at the ARC, unless on test, will result in the signal being actioned in the normal way. On discovering that a signal has been transmitted whilst the system was being tested, without notification to the ARC, the customer will be informed via auto generated incident email.

PROCEDURE FOR NOTIFYING KEY HOLDERS
Initial Ringing 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 reply 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 if all other key holders cannot be contacted.
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:
The ARC will continue attempting to contact each key holder at 20 (twenty) minute intervals. No further attempts will be made to contact a key holder where a message has been left on his/her answerphone. In respect of key holders who do not have voicemail, the ARC will continue to try and make contact for 180 (one hundred and eighty) minutes.

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. Should the site be open BusinessWatch Group will contact the site number in the first instance.

CONNECTION LOSS SIGNALS
BusinessWatch Group will only report by telephone call a total communications loss on the system. Should a connection loss be received by one of the 2 lines of communication this will be notified via email. Recurrent and/or intermittent connection signals will be placed on test until such a time that the customer resolves the issue

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 call is allowed access this will be granted.

If the caller is not listed as allowed access or cannot provide a correct password, then the operator will decline access. It is the caller's responsibility to contact the Site Manager to acquire the sights 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 BusinessWatch Group will not be able to provide access to the site unless a secondary communication path has been installed. If a secondary path has not been installed BusinessWatch Group will notify the customer on loss of connection. It is the customer's responsibility to provide access to the site in these instances.

ENVIRONMENTAL, SERVER HOSTING & SNMP MONITORING

Actions on alarms will be agreed dependent on the service being monitored and the response required by the customer. This will be agreed by RMS and the client prior to monitoring commencing and should be detailed in the relevant section at the top of this document