

This document contains information on all the monitoring and managed services we offer and forms part of our Terms and Conditions. Please refer to the relevant sections(s) for the specific services to which you are subscribing. BusinessWatch reserve the right to amend the below without consultation.

Generic Remote Monitoring Terms

About This Service

SecuriPlex UK Limited remotely monitors CCTV, Intruder, Panic and Fire systems 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, BS8243, BS8473 and all relevant standards (where applicable). All operators are vetted in accordance with BS7858:2012 and licensed by the Security Industry Authority (SIA) for CCTV Public Space Surveillance. SecuriPlex UK 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 the monitoring commissioning forms will be sent to the customer and full monitoring will commence. During the soak test period calls to the emergency services (police & fire) 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

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 Alarm Receiving Centre, Operator takes a telephone request for an Alarm Account to be placed on test the identity of the caller must be confirmed even if the Alarm Receiving Centre Operator knows the caller and the following will need to be confirmed before an account is placed on test:

- the name and address of the Account;
- the caller's name;
- the Account Code Word or the Engineer's code number.

Alarm Receiving Centre Operators 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 Alarm Receiving Centre 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 SecuriPlex UK 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 monitoring@securiplex.co.uk by a member of the site staff listed on the key holder form

PASSWORDS

SecuriPlex UK 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 SecuriPlex UK Ltd 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 regard 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. In particular they should be made aware that entry to the site outside of the normal site opening times should be 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 (SecuriPlex UK Ltd can only remotely arm CCTV systems; this cannot be done for Intruder alarms). 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. 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. Updates can only be accepted in writing and should be sent to monitoring.uk@SecuriPlex.com

RESPONSE TIMES TO ALARMS

In normal circumstances SecuriPlex UK Ltd undertakes to meet the standards for contacting the emergency services as set out in BS5979: 2007 for Category II Alarm Receiving Centres, which are:

- 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.
- For fire alarms (where the first action is to the Police or Fire Authority): 30 seconds for 90% of signals received and 60 seconds for 98.5% of signals received.
- 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
- 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, SecuriPlex UK will have access to this at all times including when the system is disarmed. This is for remote fault analysis and connection monitoring of the systems.

ENVIRONMENTAL, SERVER HOSTING AND SNMP MONITORING

Actions on alarms will be agreed dependant on the service being monitored and the response required by the customer. This will be agreed by the Business Development Manager and the client prior to monitoring commencing and should be detailed in the special instructions section at the top of this form.

Calipsa Video Monitoring Service

SecuriPlex 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 sent to the SecuriPlex ARC for analysis by an operator who will respond in the appropriate fashion

CCTV Remote 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 preset 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 that 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 ARC 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 amount of alarms is decreased, and real alarms of intruders are not hindered by the false alarms.

In the event that an activation is received from site and persons are viewed within the perimeter of the premises and verification of attendance has not been received, the RVRC Operator will issue an audio warning, advising the persons that they are being monitored and requesting they leave site immediately. After issue of audio warning, if individuals leave site the RVRC Operator will raise an incident report and enter details of event onto software provided. In the event of persons not leaving site as requested or if deemed necessary, the RVRC Operator will contact the nominated emergency key holders and request attendance. In the event that 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 Operator will immediately contact the Emergency Services and Key Holders and request attendance. The RVRC Operator 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 Client at the earliest opportunity.

PROCEDURE FOR NOTIFYING KEY HOLDERS

SecuriPlex UK 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.

SecuriPlex UK cannot enter into any commitment which would involve assuming the powers of civil Police.

CONNECTION MONITORING AND FAULT REPORTING

SecuriPlex UK 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:

Incident	Park Time	Action Required
Partial Site	30 minutes	Park site for 30 minutes (see notes on Parking an Alarm) if there is no reconnection use the relevant outcome which will generate an automatic email which will notify the customer
All Site	30 minutes	Park site for 30 minutes (see notes on Parking an Alarm) 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

SecuriPlex UK only stores images from alarms received and from the live view investigation of the alarm. These images are kept for 31 days. Where there is an incident on site SecuriPlex UK 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 Client, within a predetermined set of minutes, as advised by the customer, of the latest arming times, the RVRC Operator will identify if the system has been armed. If the system has not been armed, the RVRC Operator will contact the nominated emergency Key Holder contact to enquire as to the delay in the arming times. The RVRC Operator 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 an armed signal from the system.

EARLY TO OPEN

In the event of the remote CCTV System becoming disarmed before the appropriate time, the RVRC Operator will contact the nominated emergency Key Holder contact to verify attendance at the premises. The RVRC Operator 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 disarmed signal from the system.

INTRUDER Alarm Monitoring

ACTIONS ON RECEIPT OF ACTIVATIONS

The SecuriPlex UK response will change on the Business Day following the Test Period, to the following, unless the customer (or, where SecuriPlex UK is the maintainer, SecuriPlex UK) advises the Alarm Receiving Centre to extend the Test Period.

Type of Alarm	Action taken by SecuriPlex UK
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	Key holder Contacts

POLICE RESPONSE

SecuriPlex UK 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 SecuriPlex UK 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 Services Company* to advise the End User (and vice versa) of the current status of Police response and the responsibility of the Services Company*/End User to inform the Alarm Receiving Centre*. In the event that more than one Police alarm signal is received at the same time, only the highest priority alarm will be actioned. *In the event that these are both SecuriPlex UK, it will be the responsibility of SecuriPlex UK.

FILTERING POLICY

SecuriPlex UK 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:

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

- 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". SecuriPlex UK 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.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the Alarm Company Engineer or in some cases the End User to place Accounts on and off test with the Alarm Receiving Centre. All signals received at the Alarm Receiving Centre, 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 Alarm Receiving Centre, the Customer will be informed via auto generated incident email.

PROCEDURE FOR NOTIFYING KEY HOLDERS

Initial Ringing of a Key holder:

The Alarm Receiving Centre 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 Alarm Receiving Centre will not, on the first attempt to contact a Key Holder, leave a message on an answer-phone. However, if on a further attempt, a Key Holder is still on answer-phone, a short message will be left requesting the Key Holder telephones the Alarm Receiving Centre.

Leaving Messages if Key holder is unavailable:

The Alarm Receiving Centre 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 Alarm Receiving Centre to contact a Key Holder.

Continued Attempts to Contact a Key holder:

The Alarm Receiving Centre 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 answer-phone. In respect of Key Holders who do not have voicemail, the Alarm Receiving Centre 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 Alarm Receiving Centre 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 SecuriPlex UK will contact the site number in the first instance.

CONNECTION LOSS SIGNALS

SecuriPlex UK 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 Client, within 30 minutes of the latest arming times, the RVRC Operator will identify if the system has been armed. If the system has not been armed, the RVRC Operator will contact the nominated emergency Key Holder contact to enquire as to the delay in the arming times. The RVRC Operator 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 an armed signal from the system.

EARLY TO OPEN

In the event of the remote CCTV System becoming disarmed before the appropriate time, the RVRC Operator will contact the nominated emergency Key Holder contact to verify attendance at the premises. The RVRC Operator 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 disarmed signal from the system.

FIRE Alarm Monitoring

ACTIONS ON RECEIPT OF AN ALARM

The SecuriPlex UK response will change on the Business Day following the Test Period, to the following, unless the customer (or, where SecuriPlex UK is the maintainer, SecuriPlex UK) advises the Alarm Receiving Centre to extend the Test Period.

Type of Alarm	Action taken by SecuriPlex UK
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	Key holder Contacts

FIRE BRIGADE RESPONSE

SecuriPlex UK 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 customers local brigade.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the Alarm Company Engineer or in some cases the End user to place Accounts on and off test with the Alarm Receiving Centre.

All signals received at the Alarm Receiving Centre 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 Alarm Receiving Centre the Customer will be informed via auto-generated incident email.

PROCEDURE FOR NOTIFYING KEY HOLDERS

Initial Ringing of a Key holder:

The Alarm Receiving Centre 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 retried if all other key holders cannot be contacted.

Key holders on Answer Phones:

The Alarm Receiving Centre will not on the first attempt to contact a Key holder leave a message on an answer phone. However, if on a further attempt a Key holder is still on answer phone a short message will be left requesting the Key holder telephones the Alarm Receiving Centre.

Leaving Messages if Key holder unavailable:

The Alarm Receiving Centre 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 Alarm Receiving Centre to contact a Key Holder.

Continued Attempts to Contact a Key holder:

The Alarm Receiving Centre will continue attempts 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 answer phone. In respect of Key Holders who do not have voicemail, the Alarm Receiving Centre 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 Alarm Receiving Centre 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.

Please note that the Fire Brigade will force entry to a premises on notification of a fire alarm that may result in substantial damage to the premises should the alarm be a false signal. It is therefore imperative that a key holder lives close to the site and responds to the call promptly.

Should the site be open SecuriPlex UK will contact the site number in the first instance.

CONNECTION LOSS SIGNALS

SecuriPlex UK 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.

PANIC Alarm Monitoring

ACTIONS ON RECEIPT OF ACTIVATIONS

The SecuriPlex UK response will change on the Business Day following the Test Period, to the following, unless the customer (or, where SecuriPlex UK is the maintainer, SecuriPlex UK) advises the Alarm Receiving Centre to extend the Test Period.

Type of Alarm	Action taken by SecuriPlex UK
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

SecuriPlex UK 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 SecuriPlex UK 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 Services Company* to advise the End User (and vice versa) of the current status of Police response and the responsibility of the Services Company*/End User to inform the Alarm Receiving Centre*. In the event that more than one policed alarm signal is received at the same time, only the highest priority alarm will be actioned.

*In the event that these are both SecuriPlex UK, it will be the responsibility of SecuriPlex UK.

FILTERING POLICY

No filtering policy is applied to panic alarm signals.

UN-NOTIFIED TEST SIGNALS

It is the responsibility of the Alarm Company Engineer or in some cases the End user to place Accounts on and off test with the Alarm Receiving Centre.

All signals received at the Alarm Receiving Centre, 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 Alarm Receiving Centre, the Customer will be informed via auto-generated incident email.

PROCEDURE FOR NOTIFYING KEY HOLDERS

Initial ringing of a Key-holder:

The Alarm Receiving Centre 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-holder's 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 Alarm Receiving Centre will not on the first attempt to contact a Key holder leave a message on an answer phone. However, if on a further attempt a Key holder is still on answer phone a short message will be left requesting the Key holder telephones the Alarm Receiving Centre.

Leaving messages if Key-holder is unavailable:

The Alarm Receiving Centre will not leave messages with any person who appears to be under 16 (sixteen) years of age. Where messages have been left, this will not affect the continued attempts by the Alarm Receiving Centre to contact a Key Holder.

Continued attempts to contact a Key-holder:

The Alarm Receiving Centre 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 answer-phone. In respect of Key holders who do not have voicemail, the Alarm Receiving Centre 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 Alarm Receiving Centre 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 SecuriPlex UK will contact the site number in the first instance.

Virtual Concierge and Access Control

ACTIONS ON RECEIPT OF ACTIVATIONS

On receipt of an activation and call through to the Monitoring Centre, the Operator will view the images received, the Operator 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 rights to gain access to the premises. The operator 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 SecuriPlex UK 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 SecuriPlex UK 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 and SNMP Monitoring

Actions on alarms will be agreed dependant on the service being monitored and the response required by the customer. This will be agreed by the Business Development Manager and the client prior to monitoring commencing and should be detailed in the special instructions section at the top of this form

Call Handling

Contracted Hours of Service

The service is costed for the time of 1800 to 0800 Mondays through Fridays and all day Saturday & Sunday, as well as Bank Holidays, outside of these times the service incurs additional costs of £50 per hour. Bank holidays are those detailed on the government website <https://www.gov.uk/bank-holidays>

Call Waiting Time

There is no minimum nor maximum time for calls to be answered

Call Service

Calls are to be diverted from the customer's number to a number provided by SecuriPlex. 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 in the special instructions above, if no information is provided default information of, callers name, number, reason for phone call and site name will be taken.

The call will be passed to the relevant person by phone call and an email sent at the end of the process.

Glossary

Report Glossary

Fault Report: This report is sent to you when our Monitoring Team identifies a fault on your system. This report is sent in live time meaning that when the fault is observed by an Operator the report will be automatically created. This report requires action from you; contact the Monitoring Station to establish if the fault is still active and they can provide guidance on who to contact.

Incident Report: This report is sent to you when our Monitoring Centre has observed an event or point of special interest that they feel you should be notified of, this can include the system not being armed, staff entry to site without prior notification, a vehicle with its lights left on, or an insecure door. You will generally have been notified by telephone (or your key holders) in regards to this incident.

Intruder Seen: This report is sent to you when we have identified an intruder on your site; key-holders and the Police will have been despatched to the site.

Connection loss: This report is sent to you when connection to your site/parts of your site is lost and is notified to us by our electronic ping system. The system pings your cameras and DVRs on site; when 3 pings are unreturned we are notified of the connection loss. The report will identify if it is the whole site or certain cameras/DVRs that have lost connection. If connection is lost to all of the site it usually identifies that your broadband connection is down or the router has locked up. The first step for a whole site connection loss should be to re-boot the router and then contact the Monitoring Station to see if this has restored, if it hasn't you will need to contact your line provider. If it is not a whole site connection loss, this can point to a camera fault and should be investigated by an Engineer.

Connection Restored: This report is sent to you when connection has been restored to your site/or parts of site dependant on what failed.

Fire Alarm: This report identifies an alarm that has been triggered from the Fire Alarm System. This is a summary of the event which will have been communicated to key holders and the Fire Brigade at the time of the alarm.

Intruder Alarm: This report identifies an alarm that has been triggered from the Intruder Alarm system. This is a summary of the event which will have been communicated to key-holders and/or the Police at the time of the alarm dependant on the type of alarm and if the site has a URN or not.

Panic Alarm: This report identifies an alarm that has been triggered from the Panic Alarm. This is a summary of the event which will have been communicated to key-holders and/or the Police at the time of the alarm, dependant on the alarm.

Notification Report: This report is sent to you when our Monitoring Team identifies a note of interest that the operator has observed but does not compromise the sites security and therefore a key holder was not contacted out of hours.

Intruder, Fire and Panic Alarm Glossary

IP Fail: This identifies that the main communication path on the intruder system has failed. Intruder systems have 2 paths of communication, IP (your broadband) and GPRS (3G like on your phone) the IP is the main communication path. If this has failed it could be due to one of the following reasons

1. A temporary blip (an IP Restored alarm will be received shortly afterwards)
2. A problem on the network provider issue (your provider is carrying out maintenance)
3. Regular fails could point to a problem on the line or a router issue

What do I need to do? Contact us here at the Service Centre and we will happily provide guidance on any steps that are required.

IP Restored: This identifies that the main communication path has restored.

GPRS Fail: This identifies that the secondary communication path on the Intruder System has failed. Intruder systems have two paths of communication, IP (your broadband) and GPRS (3G like on your telephone) the GPRS is the secondary communication path. If this has failed it could be due to one of the following reasons:

1. A temporary blip (a GPRS Restored alarm will be received shortly afterwards)

2. A problem with the network provider (the network provider is carrying out maintenance)
3. Regular fails could point to a problem with the SIM Card or low signal, this can be investigated and a high gain aerial installed for low signal strengths, the SIM Card replaced if the SIM is faulty.

What do I need to do? Contact us here at the Service Centre and we will happily provide guidance on any steps that are required.

GPRS Restored: This identifies that the secondary communication path has restored.

Single Intruder Alarm: This identifies that a single detector or contact on the alarm system has been activated. This could be due to different reasons ranging from wildlife within the building, to a door/roller shutter vibrating in heavy wind. Concerns should be raised if the same detector is always activating.

What do I need to do? Contact us here at the Service Centre and we will happily provide guidance on any steps that are required.

Single Intruder Restore: This identifies that the detector has returned to the armed setting after being activated.

Confirmed Intruder Alarm: This identifies that two or more different detectors have had an activation or event. An event could be an activation on one detector and a tamper on another or two different detectors have activated. There is a time window of (30 minutes) when the system will remember that these events have occurred to automatically notify us of a confirmed intruder alarm. Confirmed intruder events are rare and will identify either a fault with the system, incorrect usage by site staff or an intruder on site.

Tamper Alarm: There are various different tamper alarm conditions that the system notifies us of, these are:

- Tamper - the detector or contact has been tampered with; this can sometimes identify a fault with that detector or contact
- Hi Res/Lo Res - this identifies a fault with the detector or contact and requires investigation by an Engineer
- Masked - the detector has been covered/blocked, this can be caused by people working in close proximity to the detector (painters/decorators) or items being placed near to the detector (stacked boxes). This can be resolved by locating the detector and ensuring there is nothing blocking it.

What do I need to do? Contact us here at the Service Centre and we will happily provide guidance on any steps that are required.

Tamper Restore: This identifies that the tamper has restored, the panel will still need to be reset, and dependent upon the tamper type an Engineer may be required to investigate the issue.

Connection to Panel Lost: This identifies that the panel has lost connection to the communication device and alarms from the system will not be alerted to us.

Connection to Panel Restored: The panel and the communication device have restored communicating to each other and alarms will be delivered to us again.

Fire Fault: This alarm triggers when there is a fault on the Fire System. This will be notified to you at the time and requires immediate action. It could point to a fire push button or smoke detector being faulty. You will need to contact your Fire Alarm Engineers urgently.

Fire Fault Restore: This identifies that the fault has restored; the panel will still need to be reset, and an Engineer will still be required to investigate.

Fire Alarm: This identifies that we have received a fire alarm from the site; we will notify key-holders and the Fire Brigade as required.

Fire Alarm Restored: The fire alarm has been acknowledged on site, investigated and the panel reset.

Panic Alarm: A panic alarm has been triggered on site.