Contents

Foreword

This document has been prepared exclusively for QVIS Monitoring customers. It sets out essential information regarding the services provided to Installer and End Users for the provision of CCTV monitoring services.

Covering both administrative and operational procedures, it is essential reading for everyone within your organisation connected with CCTV monitoring system installation, administration, servicing and management.

This document should be read in conjunction with our standard terms and conditions and, whilst we believe we have covered all aspects of service provision, the references cannot be exhaustive and our trained staff is always available to assist you further.
Information provided within this document is in accordance with BS8418; 'Installation and remote monitoring of detector activated CCTV systems - Code of Practice, and BS5979: 2007; 'Code of practice for remote centres receiving signals from security systems'.

References

This guide is based on and should be read in conjunction with the following reference documents;

- BS5979: 2007 Remote centres receiving signals from security systems
- BS8418: 2010 Installation and remote monitoring of detector activated CCTV systems - Code of practice
- BS7958: 2009 Closed circuit television (CCTV) - Management and operation - Code of practice
- BS EN 50131-2-7-1/2/3:2012 Alarm systems. Intrusion and hold-up systems
- DD243: 2004 Code of practice for intruder alarm systems incorporating alarm confirmation technology
- DD245: 2002 Code of practice for management of false alarms
- NACP20: NACOSS Code of Practice, for the Design, Installation and Maintenance of Closed Circuit Television Systems
- DISC PD 0008:1999 Legal admissibility and evidential weight of information stored electronically
- The criminal procedure and investigations act 1996
- The Data Protection Act 1998
- The Human Rights Act 1998
- SIA - Security Industry Authority

Compliance

The QVIS Monitoring ARC/RVRC fully conforms to both BS5979 for Category II ARC/RVRCs and BS8418 for the Installation and Remote Monitoring of Detector Activated CCTV Systems. Our Management Systems conform and comply with BS EN ISO 9001:2008, BS EN ISO 14001:2004 and BS OHSAS 18001:2007

Police Response/URNs (Unique Reference Numbers)

If you are installing a Security System and you require a Police response, it is essential that you:

a. Are in receipt of the full Police 'Intruder Alarm Policy' relevant to the area in which the alarm system is to be installed.
b. Appear on their Recognised List of Installers.
c. Are allocated a URN (Unique Reference Number) by the Police for each system installed.

Note 1: Where a URN has not been provided by the Installer for that system, QVIS MONITORING will not normally pass alarm incidents to Police Authorities who require a URN.

Note 2: please see ACPO Policy Appendix F for URN application (copy attached at end of document)

It is your responsibility to ensure that any change in status of a URN that will affect QVIS MONITORING's response to alarm incidents is notified, in writing, to your ARC/RVRC immediately.

We need to be kept informed of the following URN status changes:

- Level 1 Issue of new URN's and reinstatement of withdrawn URN's to Level 1
- Level 3 Withdrawal of Police Response
- Level 4 Deletion of URN's

Should a Police Authority notify us directly of a change in URN status, we will make the appropriate change to our database and inform you in writing that a change has been made.

Installer Security Codes

Certain information exchanged with an Installer may only be carried out under a strict security discipline. Upon receipt of your signed contract, we will allocate your company an account number and a Company Identity Code. You will then be invited to allocate a further code for each of your engineers, which will be matched to your unique Company Identity Code. Please ensure that Engineers are made aware of your Company Identity Code and their Unique Identification Number and that all the allocated digits are quoted.

Information or changes over the telephone by your company will only be made upon acceptance of the correct code.

End User Security Codes

End Users are required to use a Password to exchange information for alarm verification purposes. The customer may choose a password of up to 10 characters of his/her own choice. The ARC/RVRC is to be notified of the security password no later than at the point of commissioning the monitored system. NOTE: For security purposes the password should not be divulged to the Engineer.

Connection Forms

QVIS MONITORING complies with BS EN ISO 9001, and as you would expect from a conforming Security Company, data accuracy is essential. We require a ***QVM-CCTV-001_ Connection_Form*** to support every new CCTV connection. If you have any queries relating to the completion of an ARC/RVRC Connection Form, please contact your account manager on **0845 450 9994** who will be pleased to advise you.

Instructing the ARC/RVRC

Due to the security nature of instructions and the implications of an accurate response, we would ask that all instructions from Installers are made in writing on the appropriate form. Where End Users instructions cannot be forwarded via the Installer they should be received on company headed paper.
All instructions will be confirmed with the Installer as proof of receipt.
Often this will be in the form of the amended computer printout so that you can check your instructions have been interpreted to your exact requirements.

In the unlikely event of absence of confirmation, the Installer should contact the ARC/RVRC.
Emergency changes relating to Contacts, Passwords, Site and Contact Telephone Numbers or Open/Closing Times (monitored), MAY be accepted directly from End Users, provided they are registered Contacts and hold legitimate passwords and apply in writing - ***NO Verbal Instructions will be accepted.***

IMPORTANT NOTE: Audit Liability

The management of data is the most critical process within the ARC/RVRC and requires the highest level of management control by both the Installer and QVIS MONITORING.
We strongly advise that at least once per year you carry out a critical data audit, i.e. telephone numbers, URN, Contacts, etc.

QVIS MONITORING do not accept liability for any loss or error that may occur as a result of:

- Data/instructions that have not been confirmed in writing by the Installer.
- Where instructions have been submitted on non-QVIS MONITORING recognised forms.
- Where the Installer has not monitored the receipt of QVIS MONITORING data change acknowledgements or has not audited received acknowledgements for correctness.
- Where the client has input incorrect information or detail via the Web portal.

Remotely Monitored CCTV Installations

CCTV is a proven and powerful deterrent to crime, working in hand with other security disciplines to protect people, and property. CCTV Installations have been used for many years to provide enhanced surveillance of both open and secure sites.
Historically the majority of these installations have been monitored in dedicated, on-site control rooms.

Remote monitoring of CCTV is nothing new and has been offered in various ways since the 1980s. However, with the new technology available in hardware & software and high-speed broadband over fibre, remote monitoring of high quality video and CCTV has made the transition from an expensive and partially reliable service to a cost effective and efficient method of monitoring homes, businesses and commercial sites with no boundary on location and virtually no limitation on the range of services that can be offered.

CCTV surveillance systems simplistically consist of the hardware and software components of a CCTV system installed and operated to monitor a defined security zone. Unlike early electronic CCTV surveillance systems, those available today can be tailored to meet the requirements of specific sites. Matching of the equipment with the site characteristics is the crucial first step at the design stage enabling selection of the appropriate equipment. Similarly the system can only be effective if it is efficiently monitored and monitoring personnel need to be confident that activations only originate from genuine intruder activity.
Wrongly specified systems offered to clients as a cost saving alternative to manned guards severely damage the reputation of installers, monitoring companies and the CCTV industry as a whole.

CCTV Surveillance System

A typical CCTV surveillance system comprises the following equipment:

- Site Cameras - internal, external, static and/or fully functional (PTZ)
- Illumination - either standard white light or IR (Infra-Red)
- Detectors - beams or dedicated outdoor PIR/Dual-tech devices
- PA System(s) - for audio challenge etc.
- System controller - DVR or NVR
- CCTV Transmitter unit - if required, for certain sites & applications

System Configuration

Details of the site installation, camera types and locations, detector types and locations, site plans indicating camera fields of view and detection zones, entry/exit point(s), premises open/close times, type and location of DVR/control equipment, remote connection type etc. should all be provided to QVIS Monitoring using the correct forms before the system is connected to the ARC/RVRC.
Effective and reliable CCTV surveillance can only be achieved if the fundamental criteria of system configuration and design have been addressed and all potentially influencing factors carefully considered.

Successful detection of intruders is dependent on the operational efficiency of the remote monitoring system and by minimising false activations

What do QVIS Monitoring offer

ARC/RVRC monitoring centre networked to a remote CAT2 ARC/RVRC in the event of abnormal conditions, system malfunctions, temporary manning difficulties, including;

- Full technical support
- Guard Tours
- Long term stability and financial security
- Integrated Facilities Management packages for remote sites, including building system management, access control and security.
- Assistance with sales training including future trend assessment.
- Trouble shooting
- Open days & workshops for engineers and sales people
- Customer Demonstrations
- Flexible Access Control
- Advanced telemetry protocols
- Service tailored to clients' requirements
- ARC/RVRC conference facility with demo/test equipment

Construction and operation of QVIS Monitoring ARC/RVRC follow the requirements of BS 5979, Remote monitoring centres for alarm systems, and procedures are compliant with ISO 9001:2008 Quality Systems. All operational staff are recruited to the requirements of BS7858:2006+A2:2009, are licensed under SIA guide-lines and security screened (as are all personnel employed in a security environment) and are all certified CCTV operators and First Aid trained.

Expected Installation Standards

Detection systems should be installed to BS8418 and the appropriate parts of BS EN 50131. This standard provides requirements for Intrusion Systems and, in addition, for systems that provide an exterior deterrent to which the requirements of BS7992 apply.

CCTV Systems used in security applications should be installed to the guidelines provided within BS EN 50132-7 and BS8418.

Primary Objectives

- Detection and Notification
- Challenges
- Monitoring
- Identification
- Resolution (personal features, vehicle number plates)
- Recognition
- Signal Recording

Considerations

- Open/closed site
- Obstacles
- Bright lights or poor lighting
- Reflections
- Direct sunlight
- Environment

Options/Features

- Colour/monochrome
- Supplementary lighting
- Pan/tilt/zoom facility
- Access Control
- Remote Control
- IP Transmission

CCTV Design Considerations

The following statements contain key design considerations when specifying CCTV systems for compliance to BS8418, this list is not exhaustive and reference should also be made to the British Standard;

a. Ensure that sensors strictly relate to visible horizons. Sensor activations that cannot be related to a CCTV image will inevitably lead to "No obvious cause" comments.
b. Identification difficulties degrade the entire installation & monitoring efficiency.
c. Restrict sensor range to covering confines of the enclosed site, ensuring that activations are not triggered by movement from adjoining footpaths or roadways and where possible, care should be taken to ensure cameras do not overlook public areas. If cameras are triggered by passers-by or traffic outside the designed installation boundary remote intervention will be initiated which wastes valuable time resources.
d. Sensor Detection fields should ensure that unauthorised movements cross the detection zone rather than entering the field head on.
e. The negative effects of the rising and setting sun both on CCTV images, beams and PIR detectors should be carefully assessed avoiding East-West directions as far as possible. If unavoidable, the installation of secondary detectors oriented in a different direction should be considered.
f. Multiple detectors connected to a single PTZ camera that automatically drive cameras to preset locations should be individually identified by the CCTV system. Cameras should be programmed to return to a home position following completion of an event.
g. PTZ cameras should ideally be considered as multiple position fixed cameras corresponding to each preset position. It should not be possible for an intruder moving at less than 2 m/s to pass out of the field of detection before the camera can be moved to view the area.
h. Camera fields of view should be optimised to ensure that identification requirements can be met, for the purposes of verifying an event the field of view should be set to a 1.6m high target filling a minimum of 10% of the picture height. If recognition of an intruder is an objective then images sizes should be considered in excess of 50% of picture height.
i. Entry/exit routes should be viewed by fixed cameras or a PTZ camera with its' home position viewing the entry/exit route.
j. Detectors should only cause activations within the specified field of view of associated cameras.
k. Detectors and cameras should be suitable for the environmental conditions in which they are sited and there should be sufficient lighting on site to illuminate the cameras' field of view.
l. Lighting should not be positioned to directly face cameras and where timers control lighting these should be changed to and from British Summer Time.
m. Where audio challenge facilities are provided, these should be audible within the protected area and should be limited to reduce the implications of noise pollution across site boundaries.

n. Systems should be designed to initiate an event within 1 second of detection except where delays are introduced by detection within an entry/exit route.
o. The system should send continuous video images whilst under surveillance by QVIS Monitoring.
p. Video loss, tampers, line failure, power failure and failure of CCTV system within a set condition should be signalled to QVIS Monitoring.
q. Setting and un-setting procedures should ensure that unwanted activations are not caused through this activity. Therefore, automatic timed setting and un-setting carried out remotely via QVIS Monitoring may not be suitable for systems that are required to meet BS8418.
r. All of the above are as described in BS 8418

Management of CCTV Systems

Site Management of CCTV Systems that receive, hold or process data about known persons should be carried out in compliance with the Data Protection Act and Human Rights Act.
In addition, BS7958 provides supplementary guidance for owners of CCTV systems installed in places where the public have a 'right to visit'.
This includes CCTV systems where cameras view areas to which the public have access, where cameras are sited within a public area or where cameras overlook a public area. For example;

- Places in private ownership, but where the public perceive no boundary
- Places where a public service is offered
- Public footpaths, roads, etc.
- Education establishments, hospitals.
- Sports grounds, supermarket, housing areas

The Primary Requirements of BS7958 are;

Objectives and Policies

The objectives of the CCTV system should be documented in writing.
An example of a policy document is provided in Appendix A.

Documented Procedures

Documented procedures for operation of the CCTV system should typically cover;

- Organisational responsibilities in connection with the system
- Administration
- Staffing and training

Documented Procedures - continued

- Communication
- Documentation
- Control room operations, where applicable
- Access and security screening, including remote access
- Data handling and disclosure
- Observation and incident protocol
- Maintenance and faults
- Investigation, complaints, non- disclosure and disciplinary measures
- Periodic review and reporting
- Standard forms

Warning Signs

Appropriately sized signs should be placed in and around the area where CCTV cameras are located, notifying people of the existence of the cameras. These signs should also identify the owner/operator of the system and the purpose or purposes for which the data may be used so people can exercise their rights under the Data Protection Act.

Signs should be placed in the proximity of the cameras so that the public are aware that they are entering a zone that is covered by surveillance equipment. The signs should be clearly visible to members of the public.

Other Operational Considerations

The following recommendations are considered good practice and provide an outline of the recommendations provided within associated British Standards;

- Weekly checks should be made on the operational effectiveness of lighting; this can be achieved by viewing images recorded in the hours of darkness.

System Specification

Integrated communications, receiving, remote control and signal recording interfaces are available. The QVIS Monitoring preferred systems are available upon request.

Where Pan/Tilt/Zoom (PTZ) cameras are installed these should be set up to provide discrete coverage of identifiable sectors referenced to stored pre-set camera positions

Telemetry protocols should always be verified with QVIS Monitoring prior to specification.

CCTV Monitoring Contracts

Overview

Arrangements for monitoring CCTV systems must be covered by the following:

1. Standard Terms and Conditions
2. CCTV Contract
3. Operational Requirement
4. System specification comprising;
    - Insurance Requirements
    - Assignment Instructions
    - Customer Requirements
    - System Record

Schedule of Requirements & Elements

Responsibilities

The QVIS Monitoring Manager will review connections for monitoring of CCTV installations before systems are made live, it will be verified that a current Standard CCTV Monitoring contract is in place and that monitoring arrangements comply with industry standard and ACPO requirements.

Responsibilities - continued

The Installer is responsible for ensuring that all applications for connection into QVIS Monitoring are covered under the current Standard CCTV Monitoring Contract before applying to make the system live.

The Installer must also ensure that installations meet with the clients' and industry standard requirements. The Installer must notify QVIS Monitoring of any changes to the monitored installation in writing.

The End User must also ensure that installations meet with industry requirements and that QVIS Monitoring is notified of any changes to the monitored installation in writing.

Contract Documents

Standard Monitoring Agreement

A Standard Monitoring Contract details the particular conditions applied to CCTV monitoring arrangements.

Local Agreement

This document is specific to the installation to be monitored including any instruction/ amendments agreed with the end user.

The individual sections are as follows:

- Insurance requirements identifying any required indemnification and third party insurance requirements.
- Assignments identifying any transfer of rights or responsibility to others
- Customer requirements identifying the customers' instructions specific to the monitoring of the installation including the QVM-CCTV-001_ Connection_Form, and any standing instructions.
- Details of the site installation should be confirmed on the QVM-CCTV-001_ Connection_Form
- The layout of the site and camera/sensor fields of view shall be identified on the Site Plan
- The action the End User requires QVIS Monitoring to perform in the event of alarm activity shall be identified on the QVM-CCTV-001_ Connection_Form
- System Records identifying the QVIS Monitoring interpretation of the QVM-CCTV-001_ Connection_Form,
- Site Plan and any standing instructions will be retained by the QVIS Monitoring, together with a Commissioning Form indicating the outcome of system commissioning.

Connection of CCTV Systems

How to Arrange a Connection

Monitoring connections can only be made live if contractual arrangements have been formalised. If you wish to make a connection into QVIS Monitoring you need to carry out the following:

- If you do not already have a contract with QVIS Monitoring contact the QVIS Monitoring sales department (0845 450 9994) to arrange for the relevant contract package to be forwarded for signature.
- Advise QVIS Monitoring of the intended connection date.
- Confirm that the installation complies with BS8418 and BS 50132-7 or submit a signed disclaimer statement if the installation does not comply.
- Confirm that the system has been designed to permit monitoring by transmission of CCTV images to QVIS Monitoring.
- Complete a QVM-CCTV-001_ Connection_Form.
- Provide an Equipment Inventory.
- Prepare a Site Plan for integration into our records.
- Agree that on completion of commissioning, control of the system, when armed, will be solely with QVIS Monitoring

On receipt of your notification QVIS Monitoring will set up a system record file with the basic details which will allow you to carry out any necessary preliminary system testing.

Preliminary Testing

Preliminary system testing should be pre-planned and the programme agreed with QVIS Monitoring to enable a systematic review of the site installation, communications links and monitoring characteristics.

Please note that we will not retain records of preliminary testing.

Making a System Live

Before each system is made live QVIS Monitoring will require signed contract documents to be in place and all system record details must have been entered on the CCTV System Record Database including a Site Plan to enable QVIS Monitoring to process incoming signals.

Where possible system commissioning requests should be faxed or emailed twenty-four hours in advance to enable this operation to be planned into the daily work programme.
QVIS Monitoring is not responsible for any failure to carry out correct testing of the system on site. Commissioning of the system will be carried out in accordance with the procedure outlined in the Commissioning Section of this document. The Commissioning Record together with the QVM-CCTV-001_ Connection_Form and Site Plan constitutes the specific schedule to the Monitoring Contract.

Commissioning of Installations

Overview

The primary objective of commissioning is to verify that the objectives of the system design are achievable. In carrying out commissioning it is essential that each camera/sensor is activated and critical assessment made of the monitored images in both day and night conditions.

Commissioning Procedure

Prior to commencing commissioning a system, QVIS Monitoring will prepare a system record file from the CCTV Connection Sheet, Site Plan, Schedule of Equipment and the CCTV Site Commissioning Record Form.

The installer must carry out pre-commissioning tests and make appropriate adjustments or modifications to the site installation to ensure that the final commissioning process can be carried out systematically.

Any changes to previously advised details must be confirmed prior to commissioning testing.

NOTE: 24 HOURS NOTICE REQUIRED TO ENABLE FILETO BE SET UP

Commissioning Requirements

Commissioning must follow a logical progression and verify that all inventory items relevant to monitoring of the site are tested.

The appropriate sections of BS8418 should be taken into account when commissioning a system.

Commissioning of systems should be carried out as a three-part exercise:-

1. Daytime Testing

- Testing all sensors linked to QVIS MONITORING, ensuring that they are correlated with the appropriate camera, source location display should also be tested if available
- Testing all cameras linking to QVIS MONITORING
- Testing of all arming/disarming devices
- Testing of camera controls (Pan/Tilt/Zoom). Camera pre-set and remote operation should be checked for the full field of view. A reference image may be stored for finalised PTZ presets. (If preset changes are required at any time the QVIS MONITORING must be notified)
- Testing of audio links (if installed)
- All daytime tests should be carried out whilst the system is armed from site. Tests where connectivity is achieved by connecting from the QVIS MONITORING to site will not be accepted as this fails to prove connectivity on alarm and verify alignment of motion paths with those of the CCTV camera.

2. Night-time Testing

- Night checks to assess quality of supplementary lighting and image resolution. Camera tests must be undertaken with and without supplementary lighting (where applicable)

3. Seven Day Environmental Soak Testing

- During this period the system remains under test & review to permit evaluation of the effects of environmental influences and to ascertain any site trends.

ANY DIFFICULTY IDENTIFIED DURING THE COMMISSIONING PERIOD WILL BE LOGGED AND BROUGHT TO THE ATIENTION OF THE INSTALLATION COMPANY.

Acceptance of System

Acceptance of a system for monitoring is the sole discretion of QVIS Monitoring.

On satisfactory completion of the 7-day environmental soak test the system control password will be changed to prohibit control other than by QVIS Monitoring.

At this stage the QVIS Monitoring contractual responsibility commences.

QVIS Monitoring will confirm acceptance by returning an acceptance certificate to the customer.

Incident Handling

Overview

QVIS Monitoring has the facility to log communication signals, record video data, control site equipment remotely and communicate with sites using audio links, make notifications to emergency authorities (where permissible), keyholders and alarm maintenance companies.

Monitoring of CCTV installations has numerous combinations and QVIS Monitoring have standard monitoring procedures covering each major options available. The main options are:-

- Linked with approved intruder alarm
- Not linked with intruder or unapproved system
- Linked with audio challenge
- Guard Tours
- Customer Action/Notification Instructions
- Notification of emergency authorities
- Notification of keyholders
- Prescribed Action on failure to achieve contact
- Communication Link Checks

Monitoring Options

Linked with Approved Intruder Alarm System

It is anticipated that where a BS EN 50132-7 compliant monitored CCTV system is linked with a police approved intruder alarm installation, the CCTV installation will be considered as the means of visual verification. Confirmation of this status should be sought from the relevant police authority.

- On receipt of an activation our operator will dial into the site to determine a reason for the activation.
- If there is reasonable reason to believe that the activation is the result of unauthorised interference with the security of the site, the operator will advise the police of the activation as a visually verified alarm, quoting the Unique Reference Number if allocated.
- Where it is not possible to determine whether a person on site is authorised, the operator will follow the response plan.
- In instances where no reason can be determined for the activation the incident will be updated on the event log
- If a CCTV system is to be used to supplement a BS EN 50131-1 Intruder Alarm system as confirmation technology, the signalling path should conform to BS EN 50131-1 requirements.

Not Linked with Approved Intruder Alarm System or Unapproved

Where the installation is not linked to a police approved intruder alarm and/or the CCTV system is not compliant with BS EN 50132-7, the system will be considered simply as an aid to determine whether security at the site has been breached.

- On receipt of an activation our operator will dial into the site to determine a reason for the activation.
- If it is clear that an intrusion has occurred at the site, our operator will attempt to notify the specified police control room, where this telephone number has been provided by the end user.
- Should the police not accept the notification the primary contact will be notified.
- Where it is not possible to determine whether a person on site is authorised, the operator will follow the response plan.
- In instances where no reason can be determined for the activation the incident will updated on the event log.

Linked with Audio Challenge

Where audio links are in place, these can be used as a deterrent to criminals or to facilitate identification of authorised personnel. Clear instructions on the use of audio challenges should be specified. QVIS Monitoring will not accept any liability for complaints arising from the use of audio challenges in residential areas.

Clearly all personnel using the site when the system is armed should be fully aware of security password procedures.

Incorrect password exchange or failure to respond will be considered as unauthorised presence.

Guard Tours

Integrated camera position pre-sets can be programmed to enable predetermined guard tours to be carried out.

Where operator intervention is prescribed in the event of an activation, precautionary guard tours will be carried out to determine if there is any obvious reason for the activation.

If there is inferior picture quality or interference with field of view the End User will be advised

System Status

System status indicators are available giving visual display, on-site graphical plans to enable the operator to carry out activity assessments rapidly. (provided installer supplies comprehensive site plans & layout)

Access Control

It is neither realistic nor possible to monitor closed sites with personnel present on site. Where authorised site access control is a feature of the installation, it is crucial that the access control system automatically disarms the system on first entry and re-arms on last exit. QVIS Monitoring will not accept any liability for incidents where personnel remain on-site during the system set period.

Where exceptions to this arrangement are proposed prior agreement must be formally proposed and agreed with QVIS Monitoring.

CCTV Incident Monitoring

Active Incident Handling

System Status

Remote CCCTV systems are capable of being polled by QVIS Monitoring to determine whether a site is open or closed.

Alarm Images

In the event of a detected event at the remote site, the system should be capable of transmitting a sequence of stored images captured before and during the incident. The QVIS MONITORING operator views these stored alarm images before reviewing live pictures to determine the likely cause of the event.

- If no activity is determined on the alarm images, then live pictures from the same camera will be viewed to determine if movement can be seen.
- If nothing can be seen then the event will be closed down and logged in the event log as "nothing seen".
- In the event that activity can be seen then a full guard tour will be carried out of all cameras to ascertain whether any activity is present at any other part of the premises.
- It should be noted that whilst this guard tour will be carried out as a preventative measure, the system should generate an alarm condition to the QVIS MONITORING in the event of movement in the field of view of any of the CCTV cameras included as part of the system.

Live Images

Following an activation, all camera positions including pre-sets will be viewed where the alarm images or the Reference Images determine activity or changes at the protected site.

If activity is identified, the live images will be retained on-line by the operator whilst the response plan is carried out. If no cause for the alarm is identified, the event will be closed as a false alarm.

Video Loss Signals

The CCTV system at the remote site must be capable of determining and transmitting a Video Loss alarm to identify specific cameras that have become inoperable. On receipt of a Video Loss alarm the QVIS Monitoring operator will advise site contact or keyholders of the problem.

Response Plan

Specific instructions must be in place confirming the action you require us to carry out on receipt of an activation signal from the site. It is essential that these instructions are worded briefly and clearly, recognising that these instructions have to be transcribed to our database and the entry subsequently interpreted by our operators. The possibility of ambiguity in the instruction should be considered and clarification made if appropriate.

Any updates to instructions should be passed to QVIS Monitoring in writing and confirmation of receipt obtained by telephone or email
Where possible, Amendments should be kept to a minimum .

Police Intervention

Police Intervention is determined in accordance with the prevailing **ACPO policy**

URN Issuing

The issue of Unique Reference Numbers to enable Police Response to a protected site is governed by the prevailing ACPO policy. Legislation is in place at the time of writing this document and specific applications should be made to the Alarm Manager within the relevant Police Force.

URN applications are the sole responsibility of the Installation/Maintenance Company.

Risk Assessment

In determining Police Response to a protected site, the level of risk to a site must be determined.

In the event that persons are seen but no actual sign of malicious act is detected, QVIS Monitoring will contact the site/key holder to request further instructions. This route would only be taken if the enactment of the Response Plan has failed to identify the person seen or removed them from the site.

Calling Keyholders

There should be a minimum of 2 Keyholders available at all material times listed at the ARC/RVRC, unless a 24 hour key holding service is utilised in accordance with ACPO requirements. Each Key holder should have transport available and should reside within 20 minutes travelling distance of the protected premises.

- QVIS MONITORING will allow 10 rings of the telephone before terminating the call during the day (07hOO - 18hOO hours) and proceeding through the Contacts list.
- QVIS MONITORING will allow 20 rings of the telephone before terminating the call during the night (0000 - 0659 and 1900 - 2359 hours) and proceeding through the Contacts list
- In the event of all Keyholders being unavailable, QVIS MONITORING will continue to retry the Keyholders at approximately 20 minute intervals to a maximum of 3 retries.
- In the event that QVIS MONITORING has been unable to speak to an authorised Key holder, QVIS MONITORING will notify the Installer, wherever possible, that all Keyholders were unavailable.
- Answering machines or voice messages on phones are not an acceptable option for key holder response.
- Once a legitimate Key holder has been contacted, the incident will be closed. Should a Key holder decline to attend the premises it will be their responsibility to contact another authorised Key holder.
- It is strongly recommended that Contacts have mobile communications to ensure they are available at all times and to permit updates to be passed should the alarm status change whilst attending an alarm call.
- The display of the QVIS MONITORING telephone number on telephones that show 'Caller I.D.' cannot be guaranteed.

The above requirements apply to all types of alarm incidents that require site attendance.

False Alarms

General

Response times are seriously degraded if receivers are swamped by non-essential signals. Clearly, QVIS Monitoring receivers cannot be configured to differentiate between false and genuine activations, therefore we rely on the Installer and the End User to minimise the number of nonessential signals communicated to QVIS Monitoring.

Our CCTV monitoring resource allocation is based on the number of activations per week per installation detailed in the contract. We believe that this figure provides a reasonable margin for normal operation.

Multiple False Alarms

False alarms can be generated by equipment malfunction or environmental problems such as tree foliage, animals, loosely secured objects, passing traffic etc. Many of these activations are spasmodic and it is frequently difficult to determine a cause. Installations generating repeated false alarms are assessed routinely and offending components should be disabled where it is not possible to rectify the problem. A standard disablement procedure applies in these instances permitting the QVIS MONITORING to direct resources to priority monitoring tasks.

Disablement Procedure

Where an installation generates excessive numbers of activations we will notify the end user and request that the problem is addressed (or advise that the camera/sensor requires to be disabled).

The Camera/Sensor Disablement Assessment Criteria are as follows;

- Any camera/sensor generating more than four non-intruder activations in a one hour period will be disarmed until premise opening time and the subscriber (or representative) advised.
- If the installation continues to communicate false activations the subscriber will be notified of our intention to disable the camera/sensor until the problem is rectified.
- Formal notification will be made in the event of malfunctioning equipment or suspected environmental effects.
- The notification confirms actions taken and should also be used to confirm re-enablement authorisation and monitoring status of the site.
- Continuing false alarm generation requires remedial action and if the site problem is not rectified an additional charge will be made for each activation in excess of the agreed contractual amount.

Disabling a Camera which initiates "No Video Signals"

- Where necessary the camera No Video Signal message can be disabled leaving the sensor on line.
- This will only to be carried out after;
- Signals are received from a particular site indicating that the camera/sensor cannot transmit images or transmits multiple false alarms and that these have been assessed as not being due to malicious action.
- An Installer Engineer or Subscriber has been contacted and advised of the situation, authorises us to turn the camera/sensor off; and all details and actions have been logged including the authorisation and the reason.
- Confirmation of disarming is faxed or emailed to the Installer by using a fault report.

Note: Following camera/sensor disablement it is the responsibility of the Installer to confirm instructions to re-enable cameras/sensors.

Each installation should be covered by a formal maintenance service agreement with an approved installer/maintenance company.
This service agreement should provide for both preventative and corrective maintenance.

Remote Access to Site

Preventative Maintenance

A planned programme of preventive maintenance and system checks prescribed in NACP20 and BS8418 should be in place.
The programme should consider the overall performance of the installation, review activation reports and camera disablement notifications.

Where the overall effectiveness of the system is dependent on the ability of a QVIS Monitoring operator interpreting CCTV images, a review should be carried out in relation to the end users current requirements, installed equipment and operational history. Assessments of monitoring capability should ideally be carried to a predetermined schedule, which should be used to formalise the findings.

This final part of the assessment is normally in the form of a "Walk Test"

Corrective Maintenance

QVIS Monitoring is available to assist in investigations and proving tests. These can be in the form of a "Walk Test" or other agreed pre-arranged routines. If appropriate, formal records can be arranged.

Walk Testing

Routine commissioning or maintenance testing may require an "Engineers Walk Test." End Users may also require a "Customers Walk Test" as part of their own procedures.

Full records of the walk test should be kept by both site and QVIS Monitoring preferably using a Site Commissioning Record Form.

The records should be agreed and include site, engineer/site representative, password, day and date and extent of test.
In the event of any fault being identified a record of the findings will be communicated to the Installer.

In order to ensure that testing is carried out in controlled conditions the following conditions should apply;

Engineer Tests

Engineers will need to be registered as an Authorised Engineer with QVIS Monitoring. The Engineer should specify the site, the extent and sequence of testing, giving as much notice as possible to enable the system record to be brought up.

- Engineer must demonstrate authorisation by password etc.
- Ideally the test should follow the pre-arranged sequence.

On completion of the test, the Operator and Engineer should agree the record of test.
At this point live images will be checked against the Reference Images to ensure that the system is compliant to the specification at Commissioning. Where authorised by the customer, new Reference Images will be stored to reflect changes.

Engineer should advise the Operator that he is leaving site and if appropriate instruct that the site should be made "live".

Customer Walk Test

Customers may undertake a walk test of the system by prior arrangement with the QVIS MONITORING. Site Representative should identify himself/herself by name with a relevant authorisation password.

Site Representative should advise the extent and purpose of the Site Walk Test specifying those sensors, cameras and audio points to be visited.

Records and Reports

Overview

The principal records retained by QVIS Monitoring are;

- Activation Logs
- CCTV images
- Actions / Notifications / Interventions
- Voice Communications (not audio announcements)
- Disablements
- System Records including changes to customer instruction for notifications

Detail of Records

Activation Logs

The time of receipt of initial activation and perceived causes will be logged against all activations as part of an auditable activation history. A prescribed menu will be used to classify causes. The time that the session closed down is also logged.

CCTV Images

All images received at QVIS Monitoring as a result of activation are recorded in the site alarm event log. These images are stored in digital form on HDD. Video records are retained for a minimum period of 31 days.

Actions/Interventions

Whenever an assessment of activations is carried out, any remote operation of site equipment is logged. All operator interventions are logged including camera/sensor Omission and Re-instatement.

Voice Communications

All inbound and outbound telephone calls are recorded.

Notifications

Notifications of site, keyholders, emergency authorities and Installer are logged, and where applicable allocated incident numbers recorded.

Deactivations

Operators have the facility to carry out Omission and Re-instatement of cameras and detectors where these are causing problems that are affecting the overall efficiency of QVIS Monitoring.
Where Omission is necessary the appropriate notification will be made.

System Records and Changes to Instructions

Connection details are retained and changes to monitoring instructions are logged.

Activation Reports

Activation logs and associated actions taken are retained for six months. Summaries are forwarded daily to Installer.

Reports

The following reports are available dependent upon the chosen service level;

- Activation Logs: Daily summaries giving time of receipt, camera activated and action taken.
- Guard Tour Abnormal Incident Report: In the event of any abnormal observation during a routine check on an installation the subscriber will be advised.
- Camera/Sensor Disablement Notifications: Confirming disarming of cameras/sensors when fault conditions are suspected.
- Video Image Copies: Where appropriate copies of video images received at the QVIS MONITORING can be provided. A small administration charge may be made in accordance with the Data Protection Act.

Quality Testing

Quality Checks

The following quality checks will be pro-actively carried out by QVIS Monitoring subject to service level agreement;

Weekly System Health Checks

If a system has not activated within a seven-day period QVIS Monitoring will, where possible, remotely access the system when it is reflecting set status. Each camera view will be accessed to ensure that a clear image quality can be obtained in line with the Reference Images stored at point of Commissioning. QVIS Monitoring will notify the customer by exception via fax or email if a fault is detected.

Live Incident Quality Checks

If during the handling of an Event the quality of an image is identified as poor, a fixed format notification will be issued to the customer advising them of the nature of the problem and requesting remedial action be taken.

Critical Data Omissions

If during the handling of an event critical data that is required to complete the response plan is unavailable or inaccurate (e.g. key holder no longer valid) a fixed format notification will be issued to the customer by fax or email requesting the supply of the missing data.

Service Levels

Incident Response Time

Alarm activation images will be viewed, wherever possible, within the timescales defined within BS8418;

- Within 90 seconds of their arrival for 80% of activations received
- Within 180 seconds of their arrival for 98.5% of activations received

It should be noted that excessive false alarms will lead to a reduction in service levels.

Local System Fault Reporting

When faults are detected on the system, customers will be notified by fax or email the next working day.

Telephone Response

Wherever possible the monitoring station will ensure that;

- 80% of calls are answered within 15 seconds
- 95% of calls are answered within 45 seconds

Incident Investigation

Incident Investigation Requests

Installer should formally request a detailed incident investigation, such as a request for supply of video/data information, using a Complaint/Query Confirmation Form quoting:

- Reference Number
- Site Name
- Time & Date of incident
- Information required
- Reason for information request
- Value of any potential claim

Incident Investigation Reports

Our response will provide;

- Verbal acknowledgement and interim response within 24 hours
- Written response including video review with video print out of any suspicious activity normally within three working days (subject to approval by the companies' legal representative).

Video Record Retention

Recordings covering periods under investigation will be quarantined for six months from date of receipt of incident investigation request.

Customer Complaints

Complaints received either in writing or verbally will be dealt with as follows;

- Installer should contact the Manager/ Supervisor with information regarding the complaint.
- Complaints from End User should preferable be received in writing.

QVIS Monitoring provides an interim verbal report within one twenty-four hours and a full written report normally within three working days, subject to the conditions detailed above. All communication will be routed through the holder of the monitoring contract unless formal instructions are given to the contrary.

Event Reporting

All event recorded within a closed period will be reported where possible, by fax or email to the customer's nominated contact within the next working day.

New Site Connection

A new site will be set up for commissioning within one working day of receipt of details from existing customers.

Data Protection Act

Compliance with Data Protection Act

QVIS Monitoring is bound by the Office of Data Protection Registrar Code of Practice and is registered with the ICO registration number: ZA026308

In the interests of our customers, the following statements that refer directly to CCTV monitoring of premises have been extracted for information within the DPA regulations.

If it is not possible to prevent periodic surveillance of areas accessible to the general public (e.g. public footpaths, adjacent roads etc) or monitoring carried out of garage forecourts the appropriate signage must be exhibited. This is the occupier's responsibility.

Where QVIS Monitoring can control cameras, the fields of view should be restricted to ensure that they do not operate outside the scheme boundary.

Where there could be a requirement to provide images to third parties there should be prior agreement from the occupier in writing.

A statement complying with the seventh Data Protection principle - to ensure that personal data on individuals whose images have been captured will be treated with respect will cover any response to a request for copies of video tapes.

Further Reference

For further information please refer to the Office of Data Protection Registrar Code of Practice for users of CCTV and similar surveillance equipment monitoring spaces to which the public have access.

SAMPLE POLICY STATEMENT

CCTV System Policy Statement

1.0 Owner

<Company name> has in place a CCTV surveillance system on these premises.
The system is owned by <Company name>. The <job title of person responsible for CCTV system> is responsible for operation of the system and for ensuring compliance with this policy and may be contacted as follows:
<Job Title>
<Address>
<Telephone>
<Email>

2.0 The system

The system comprises: <insert basic details of the system - i.e. Static cameras; Pan Tilt and Zoom cameras; Monitors: DVRs, NVRs; Public information signs; >.

Cameras are located at strategic points of the premises, principally at <insert location of cameras>. No camera is hidden from view and all are prevented from focussing on adjoining premises and public areas.

Signs are prominently placed at strategic points to inform staff, visitors and members of the public that a CCTV installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

3.0 Purpose of the system

The system has been installed with the primary purpose of reducing the threat of crime generally, protecting the premises and helping to ensure the safety of staff and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- deter those having criminal intent
- assist in the prevention and detection of crime
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order

The system will only be utilised for the purposes stated above.

4.0 Live and Stored Images

Images captured by the system will be monitored and recorded by staff having responsibilities for site security and in addition during set periods images may be viewed and recorded by the ARC/RVRC at the address below;

QVIS Monitoring Ltd
36 New Lane
Havant
Hampshire P09 2JL

Tel: 0845 450 9992
email: info@qvismonitoring.co.uk

Access is restricted to authorised members of senior management, QVIS Monitoring duty personnel and management, police officers and any other person with statutory powers of entry.

5.0 Administration and Procedures

It is recognised that images are sensitive material and subject to the provisions of the Data Protection Act 1998; the Manager responsible for the system will ensure day to day compliance with the Act. All CCTV recordings will be handled in strict accordance with this policy and recorded images will be retained for a maximum of 31 days, excepting any specific images that are identified as providing evidential information under the purposes of the scheme, in which case they will be held until completion of any investigations or prosecutions.

6.0 Staff

All staff having access to the CCTV system are made aware of the sensitivity of handling CCTV images and recordings. The Manager responsible ensures that all staff are fully briefed and trained in respect of their responsibilities from the use of CCTV, and licensed under the SIA Public Space Surveyor Guidelines. Training in the requirements of the Data Protection Act 1998 is given to all those required to have access to CCTV recordings.

7.0 Recording

Each recording is uniquely identified and all activities associated with it are recorded in the Recording Log up to and including its final erasure and disposal. The Recording Log is kept secure and access to it is only available to relevant members of staff.

ACPO Policy Appendix F

ACPO Policy Appendix f follows: