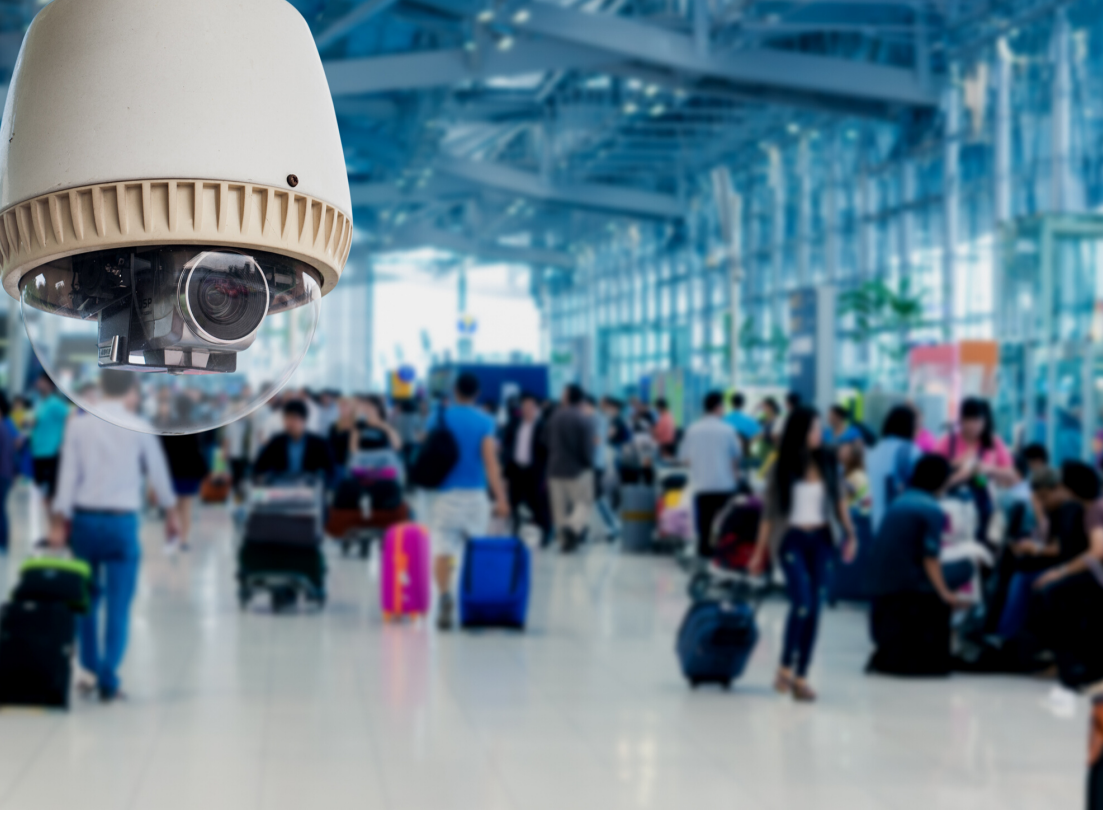
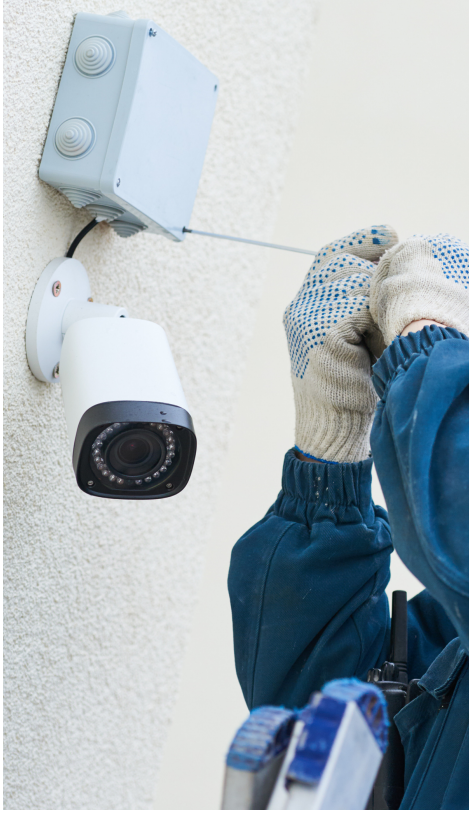
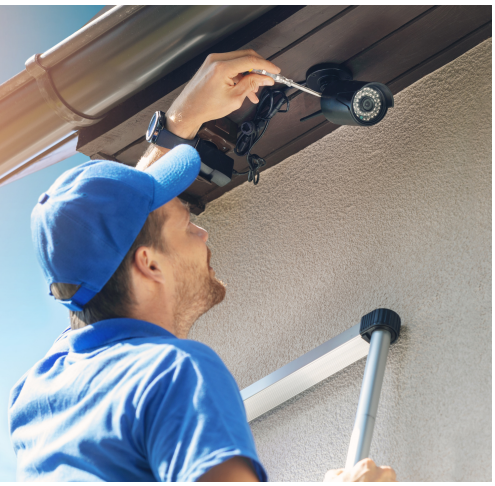






Maintenance of Video Surveillance Systems (VSS)
code of practice

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association

Acknowledgements

The BSIA acknowledge the assistance given by the following member company in the development of this guide: Dave Stones – Secure One

For other information please contact:

British Security Industry Association

01905 342 020
info@bsia.co.uk
www.bsia.co.uk

Contents

0. Introduction

Effective and regular maintenance of a Video Surveillance System (VSS) is essential to ensure that the system remains reliable at all times. Regular maintenance by the maintenance company and effective failure reporting by the user will enable potential problems to be identified at an early stage so that appropriate action can be taken.

It is important to remember the significance of cybersecurity in any maintenance programme, cybersecurity relies on ongoing support to ensure the resilience of the VSS system and the individual components (or equipment) that comprise the VSS system. Not all VSS systems have a cyber exposure but for those systems that do, it is vitally important to ensure that there is an effective security update programme. For further information on cybersecurity see BSIA Form 342, *Installation of safety and security systems cybersecurity code of practice*.

Maintaining a VSS system is preceded by proper planning, design and installation of such systems. See BSIA Form 109 for further information.

Whilst maintenance of VSS systems in the main may be voluntary, there are some legislative requirements introduced by Government that may impact on the ongoing maintenance or indeed need for a VSS system. In the UK, The Home Office and the Scottish Government have recognised the potential for appropriate and effective use of VSS systems. There is regulation included in the Protection of Freedoms Act: 2012. One of its legislative requirements for public space VSS systems is the development of the Surveillance Camera Code of Practice, which is founded on 12 guiding principles to ensure VSS systems are appropriate and proportionate. Cross references to the 12 Guiding principles of the Surveillance Camera Code of Practice are reproduced in Annex D for information.

For Scotland, the Scottish Government published A National Strategy for Public Space in Scotland in 2011 which includes a standards and regulatory framework for public space VSS systems.

1. Scope

This code of practice provides recommendations for the maintenance of VSS systems used in all security applications. It should be used to supplement systems installed and maintained in accordance with the following published standards:

BS EN 62676 *Suite of International (IEC) standards*

BS 8418 *Installation of detection activated VSS systems – code of practice*

2. Definitions

2.1. Definitions

2.1.1. Customer

Person or organisation employing the services of a maintenance company to carry out maintenance of the VSS system.

Note: *A customer may also be the user.*

2.1.2. Maintenance company

An organisation that provides a service for the maintenance of the VSS system.

2.1.3. Technician

A person employed by the maintenance company to carry out maintenance of the VSS system.

2.1.4. User

The person authorized by the customer utilizing the VSS system for its intended purpose.

Note: *A user may also be commonly known as an "operator" of the VSS system.*

3. Maintenance company requirements

It is advisable that VSS maintenance should be carried out by the installing company, but whatever arrangements are made, the company appointed as the "maintenance company" should have the necessary resources, including spare parts, to meet all the recommendations of this code.

Note: *This recommendation does not place an obligation upon customers who purchase their VSS systems to have them maintained by the installing company; maintenance is a matter of agreement between the customer and the installing company or a separate maintenance company. Some VSS systems do require a maintenance agreement. See Clause 4 Maintenance agreement.*

The preservation of the security of the customer's equipment and all data pertaining to the customer's installation is of the upmost importance and steps should be taken to ensure the safe custody of this within the maintenance company.

Note: *The maintenance company should be aware of the requirements of Data Protection Legislation as it applies to VSS and the Information Commissioner's Office (ICO) In the picture: A data protection code of practice for surveillance cameras and personal information. See: ico.org.uk*

The maintenance company should ensure that vetting of employees, who have access to customer equipment and/or data, is carried out in accordance with **BS 7858** - *Screening of individuals working in a secure environment – code of practice.*

Where employees are involved in BS 8418 systems then a police conviction check (**NPCC Police Operational Advice and Security Industry Requirements for Response to Security Systems – appendix C**) will be required or in the case of those companies working in the Police Scotland region then a Disclosure Scotland certificate will be required.

There should be a method to identify all employees to external parties, e.g. this could be achieved via the use of an identity card (where this is utilised the card should include a photograph and signature of the bearer, the company's name and a date of expiry).

Each technician employed by the maintenance company should carry a range of tools, test equipment, suitable spare parts and other equipment or plant to enable them to perform their functions satisfactorily. Specialist tools, test equipment and plant should be available for deeper more complex investigation, as necessary.

The maintenance company should be resourced to ensure that the recommendations of this code of practice can be met at all times. The following factors should be taken into consideration:

- The number of installations to be maintained.
- The complexity of the installations.
- The geographical spread of the installations in relation to the maintenance company, its office locations and the number of technicians available to carry out the work.
- The method of calling out technicians outside normal office hours to meet contracted requirements, where applicable.

Technicians should be adequately trained on VSS systems and the products and equipment they are likely to support during the course of their work. Ongoing training should be provided whenever deemed necessary.

4. Maintenance agreement

Where a maintenance agreement is to be arranged, the agreement should be between the maintenance company and the customer.

Note: *Agreements may be needed for a variety of reasons, such as requirements under the NPCC Police Operational Advice and Security Industry Requirements for Response to Security Systems document for detection activated VSS systems (to obtain a Police URN). Or they may be needed where images from the system are used for evidential purposes.*

The maintenance agreement should be based on the VSS system specification (and operational requirements, where identified) drawn up by the installing/maintenance company in agreement with the customer. This specification should include the location of all equipment installed; the coverage and any limitation of surveillance of all cameras and any specific privacy requirements. The customer should be provided with a copy of the specification, should also be advised to store it in a secure location on site and that it should be made available to the maintenance company technician during visits.

The maintenance agreement should also contain the following provisions:

- The price and the period of support to which the agreement applies; start and end dates for the contract; the action required for renewal; labour rates for chargeable visits.

- The equipment that is/is not covered by the agreement including consumable/perishable items.

- Any services not included in the agreement e.g. civil works, whether parts are included in the quoted cost or are to be charged separately. Any fault causes which will give rise to a chargeable visit – e.g. vandalism, act of God.

- The operating hours (and days) during which faults can be reported. The operating hours (and days) during which faults will be responded to.

- The time that the maintenance company will take to respond to faults. The time that the maintainer will take to repair faults (customers and the maintenance company should consider that the time taken to respond is often of less consequence than the time taken to repair faults). Whether the customer needs to hold spares on site in order for a repair time to be guaranteed. Whether there are any elements of the system that require an enhanced or escalated response – consider the impact of the loss of one camera versus the loss of the whole system or a significant part of it.

- The means available for the customer representative to report faults including telephone numbers and/or email addresses - escalation procedures if applicable. Dependencies – e.g. if the customer needs to provide an internet connection for the provision of remote support.

- Whether there are to be regular meetings to discuss maintenance and, if so, at what frequency. Any performance reports that will be provided and at what intervals.

- Cybersecurity responsibilities, i.e.
  - how security updates will be notified and applied to the VSS system.
  - customer controlled IP network and components (or equipment) that will be the responsibility of the customer for security updates.

5. Maintenance requirements

5.1. European and International standards requirements

BS EN 62676-4 provides requirements for the maintenance of VSS systems. This code of practice provides additional recommendations for the maintenance of VSS systems and provides examples of the type of documentation required to be used by the maintenance company.

It is recognised that for VSS systems that are within the scope of the Surveillance Camera Code of Practice, principle 8 requires that the use of approved technical and competency standards be used. Standards such as those listed above are likely to feature in the Surveillance Camera Code of Practice and will be detailed on the **Surveillance Camera Commissioner's** website.

See **Annex D** for a list of the Surveillance Camera Code of Practice principles.

5.2. Types of maintenance

There are three types of maintenance that are required to be carried out on a VSS system.

5.2.1. Preventative maintenance

Planned maintenance of a system, carried out on a scheduled basis.

5.2.2. Corrective maintenance

Emergency maintenance of a system, or part thereof, carried out in response to the development of a fault.

5.2.2. Customer and user maintenance

Basic maintenance/fault reporting tasks, as detailed by the maintenance company, carried out by the system manager and/or system user.

Types of maintenance are described in detail in sections 6, 7, 8 and 9.

6. Preventative maintenance

6.1. Recommended frequency of maintenance

A preventative maintenance visit allows the technician to carry out a complete audit/check of the VSS system, the documentation associated with the system, and the training requirements of users.

The VSS system should receive at least one preventative maintenance visit each year. However, additional maintenance visits may be required depending on the complexity of the system, the environmental conditions, and the need to change 'perishable items' e.g. wiper blades, batteries etc.

Note: *These preventative maintenance visits are additional to any corrective maintenance visits which may be required.*

VSS systems installed in accordance with BS 8418 are subject to preventative maintenance visits per annum dependent on their system type. See BS 8418: 2021 for frequencies specified.

6.2. Preventative maintenance report

The technician should complete a maintenance report whilst carrying out preventative maintenance of a VSS system.

The report should list any deviations of the system from the fully functional state and should list relevant comments about the system e.g. Camera 1 replacement dome cover required at next visit.

The report will help the customer and / or user to monitor the reliability of the VSS system to ensure it continues to meets its original purpose, remains up to date with latest software (cyber secure) and will assist the budgeting of any replacement parts required in the future.

A copy of the report should be made available to the customer and/or user on completion of the maintenance.

Note: *Some reports and checklists may be on electronic media and therefore may be presented to the user for acceptance and sent to them after the visit, e.g. by email, post etc.*

A sample of a preventative maintenance report is shown at **Annex A**.

7. Corrective maintenance

7.1. Response time

Corrective maintenance calls are the emergency maintenance of a system, or part thereof, carried out in response to the development of a fault or damage. Suitable communication should be used to ensure the customer and/or user can be informed of expected arrival times to site.

Note: *Response times should be a feature of the contract/maintenance agreement.*

7.2. Corrective maintenance report

On completion of corrective maintenance, the technician should complete a maintenance report and give a copy to the customer and/or user.

A sample of a corrective maintenance report is shown at **Annex B**.

Note: *Some forms and checklists may be on electronic media and therefore may be presented to the customer and / or user for acceptance and sent to them after the visit, e.g. by email, post etc.*

8. Customer and user maintenance

8.1. General

Whilst it is recognized this code of practice should not place requirements on the customer, it is important that the customer is aware of the importance to provide user maintenance to the VSS System.

The customer should also conduct a periodic review of the VSS system's effectiveness to ensure it is still doing what it is intended to do. Good practice would also suggest the 12 guiding principles in the Surveillance Camera Code of Practice be followed to ensure the system remains fit for purpose. See **Annex D** for a list of the principles.

Where the VSS system relies upon a third party IP network to function correctly (for example the customer's existing IP network, or an IP network under the control of the customer, or customer's sub-contractor) then the customer should be responsible to ensure the cybersecurity of that network.

The maintenance company should consider the following recommendations for inclusion in any agreement with the customer.

8.1.1. Customer

The customer/user should ensure all fault reporting on the VSS system is undertaken in a methodical and timely manner. The following should be considered:

a) Ensure all users are trained on a regular basis in the actions to take in the event of a system fault.
Note: *annual training of users is recommended.*

b) Ensure faults are reported as soon as possible after they are discovered, and that details are entered in a fault reporting book.

c) Inspect the fault reporting book weekly to ensure all faults are dealt with efficiently and effectively.

d) Decide if the fault can be corrected in-house or whether the technician is required.

e) Liaise with the maintenance company when a technician is required.

f) Ensure the technician has access to site, specification and equipment at an agreed time and date.

g) After repair has been carried out, sign and keep a copy of the corrective maintenance report for the system record.

h) Sign off the work from the fault reporting book. A typical fault reporting procedure is shown in **Annex C**.

i) Where the VSS system utilises an IP network (or part of an IP network) that is under the control of the customer then it should be clear who will ensure the cybersecurity of that network and ensure security updates are applied (this could be the responsibility of the customer or maintenance company).

8.1.2. VSS system user

8.1.2.1. Checks carried out during each shift

The system user should normally be the first to notice a fault with the VSS system. To ensure the system operates effectively the user should:

a) Check the fault log at the start of a shift to see if there are any outstanding faults on the system.

b) Check the operation of the system at the start of a shift and report any faults to the system manager. In addition, details of the fault should be recorded and appropriate action taken.

c) If the fault is not cleared during the user's shift, the next shift should be informed of the fault and what corrective measures, if any, have been actioned.

8.1.2.2. Additional checks carried out by the system user

a) Clean the monitor screens weekly.

b) Clean the control surfaces weekly.

c) Ensure recording facilities are operating correctly (agreed between the customer and maintenance company).

d) Clean any hardware air vents monthly.

e) Carry out any other functions recommended by the maintenance company.

9. Remote maintenance

It is likely that some support may be given to the customer/user remotely. This may take the form of remote diagnostics/support or remote maintenance, be it corrective and/or preventative. Whilst these have some significant advantages, such as limited system down-time and perhaps call-out costs, it is not without its potential vulnerabilities such as network security and data protection issues which should be a key consideration.

There should be an agreement in place (service level or otherwise) for the VSS system to cover the following:

a) Agreement on what level(s) of access/permissions is granted to the maintenance company to log onto the site VSS system. This should include, if it is in response to an incident, a request from the customer a and/or user or if it is part of a preventative maintenance agreement.
b) A response plan that specifies what action to take when certain types of event occur. For example, loss of communication with the site control equipment isolation of an alarm, switch off/on ancillary equipment, reset or restart the VSS system or notify nominated persons.
c) Actions to be taken in the event that a data breach becomes known to either party.
d) There should always be an audit trail for remote user activity.

Note: *Software is available that can monitor the status of control equipment on site such as DVR / NVR or transmission equipment, which can inform the remote centre of loss of signalling, video loss from cameras, provide time synchronization etc*.

Such software may also be able to provide an 'at a glance' view of system status highlighting any current issues.

10. Documentation

The following documentation is required to be held by the maintenance company providing maintenance to the VSS system:

a) System "as fitted" specification*
b) Handover check list/completion certificate
c) Maintenance agreement
d) Preventative maintenance report (see **Annex A**)
e) Corrective maintenance report (see **Annex B**)
f) Installed equipment manuals*

*A copy of these documents should be held on site.

The maintenance company should comply with the data protection legislation as it applies to them with regard to customer data held.

11. Perishable items

The maintenance company should hold a record of all components with limited lifetime, and components should be replaced when required. Consideration should also be given for any components held by the customer, which may also be subject to similar limits.

Annex A: Example of a preventative maintenance report

Preventative maintenance report for VSS systems

Company Name:_____ Company address:_____ Customer:_____

Site:_____ Site ref:_____ Date:_____

CHECKS TO BE MADE	Confirm checked	Comments
Check the number and type of cameras, including lenses, are in accordance with the specification and any amendment.		
Check visual/audible indications are functioning correctly.		
Check warning notices/labels are still in place.		
Check all cables and fixings remain properly supported, undamaged and showing no undue signs of wear.		
Check for sound physical fixings of all equipment including loosening or corrosion of supports and fixings including towers and brackets.		
Check all glands and seals on external equipment to ensure no ingress of water into the equipment.		
Cameras, lens, covers and housings have been cleaned where necessary to ensure nothing obscures the field of view.		
Check the picture quality of each camera and correct monitor selection.		
Check all automatic and remote control camera functions are satisfactory and that camera movement and fields of view are free from obstruction and any privacy masking zones are still in place.		
Operation of all monitoring, switching and recording equipment (including time synchronisation) is satisfactory.		
Function of all interfaces with alarms is satisfactory including correct triggering of alarms.		
Operation of supplementary lighting is satisfactory.		
Check that the performance of the system(s) continues to meet the agreed specification/ operational requirement according to the periodic test scheme agreed with the customer.		
Where necessary, check that software is up to date and that all security updates have been applied.		

Additional comments: incl. any further recommendations to the VSS system:

Equipment left disconnected
The system has been left in full working order, except for the disconnected item(s) listed below:
Item(s) disconnected: _____

Permanent OR temporary OR put on test

Planned reconnection date (if known): _____

Revisit
Is a revisit required? Yes/No

If YES, state why in the comments section above and give details below of any agreed arrangements:

Revisit date: _____ Time:_____ am/pm

Technician's name: _____ Tech. Sig: _____ Date: _____

I accept that the work carried out is to my satisfaction and confirm that I am authorised to sign on behalf of the company and / or subscriber. I have also been made aware of any disconnected equipment and arranged revisit as listed above.

Customer representative's name: _____ Signature: _____ Date: _____

Annex B: Example of a corrective maintenance report

Corrective maintenance report for VSS systems

Company Name:_____ Company address:_____ Customer:_____

Site:_____ Site ref:_____ Date:_____

Reported fault (by the customer / user):

Fault category: Customer / user related **[ ]** Company related **[ ]** Other **[ ]** Specify:

Action taken (by the Technician) comments:

Materials used:

Chargeable: YES **[ ]** NO **[ ]**

Equipment left disconnected
The system has been left in full working order, except for the disconnected item(s) listed below:

Type of disconnection: Permanent **[ ]** Temporary **[ ]** Subscriber to notify

Planned reconnection date (if known): _____

Revisit
Is a revisit required? YES **[ ]** NO **[ ]**

If YES, state why in the comments section above and give details below of any agreed arrangements:

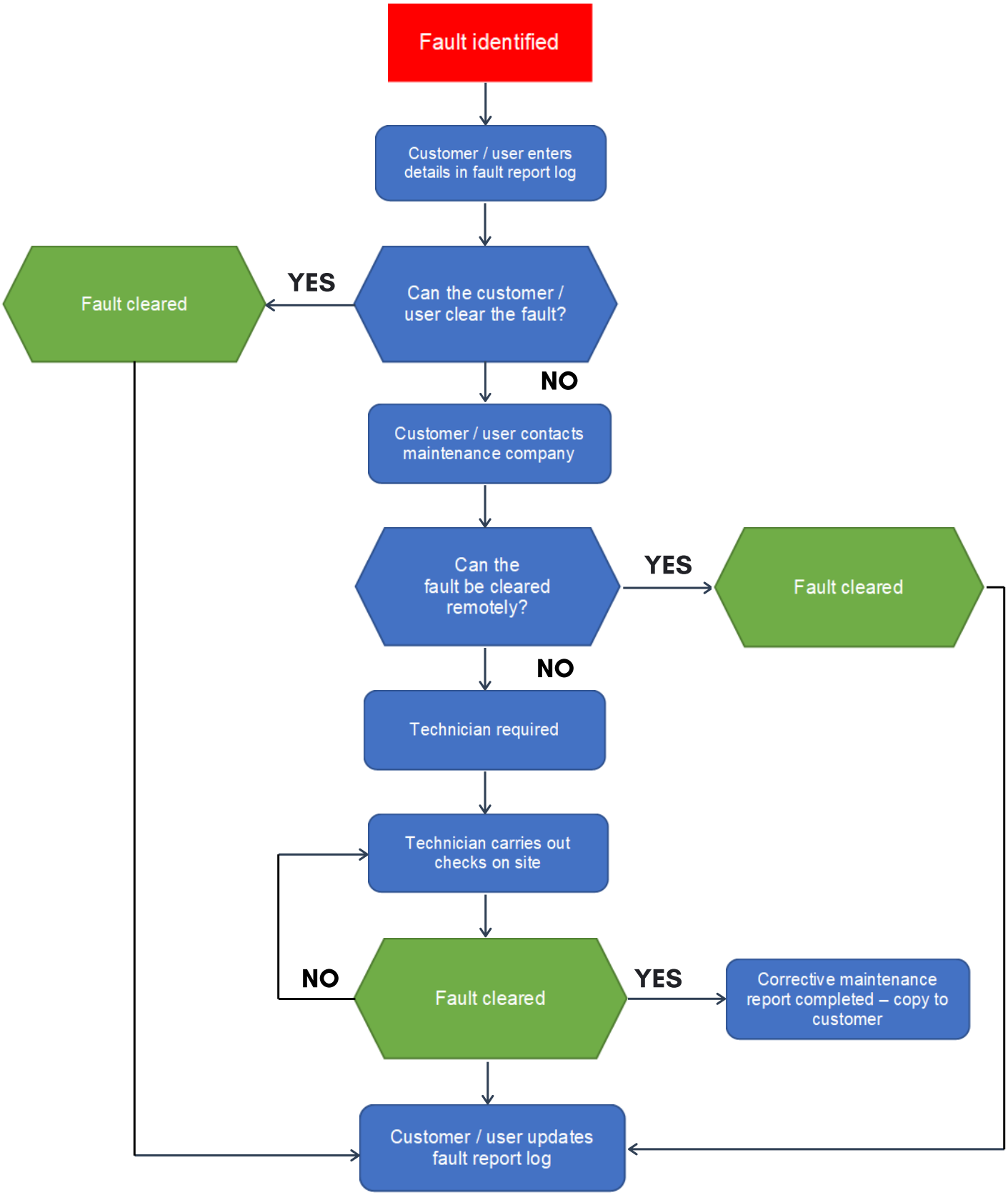
Revisit date: _____ Time:_____ am/pm

Technician's name: _____ Tech. Sig: _____ Date: _____

I accept that the work carried out is to my satisfaction and confirm that I am authorised to sign on behalf of the company and / or subscriber. I have also been made aware of any disconnected equipment and arranged revisit as listed above.

Customer representative's name: _____ Signature: _____ Date: _____

Annex C: User fault reporting procedure



Annex D: Surveillance Camera Code of Practice – 12 Guiding Principles

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8.Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

About the BSIA

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

VSS has had a profound impact on crime prevention and detection. The UK leads the way in the application of VSS and its use is wide-ranging, encompassing facial-recognition technology, remote video monitoring, video smoke detection, mobile systems and Automatic Number Plate Recognition as well as many other functions.

To provide guidance and simplification in the complex area of VSS, the BSIA is very active in the European & International standards arena's and also develops its own guides and codes of practice where currently standards do not exist.

The VSS section encourages debate on new developments and concerns, such as digital video evidence and facilitating communication protocols between different manufacturers' products. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, users, the Police, inspectorates and insurers.

The section also works with Government on these issues.

VSS must be operated responsibly in order to respect citizens' rights and maintain public confidence. Laws such as the Data Protection Act have an important role to play in achieving this. BSIA VSS companies drive best practice in this area and can provide advice on how VSS users can adhere to the relevant legislation.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

British Security Industry Association

01905 342 020
info@bsia.co.uk
www.bsia.co.uk