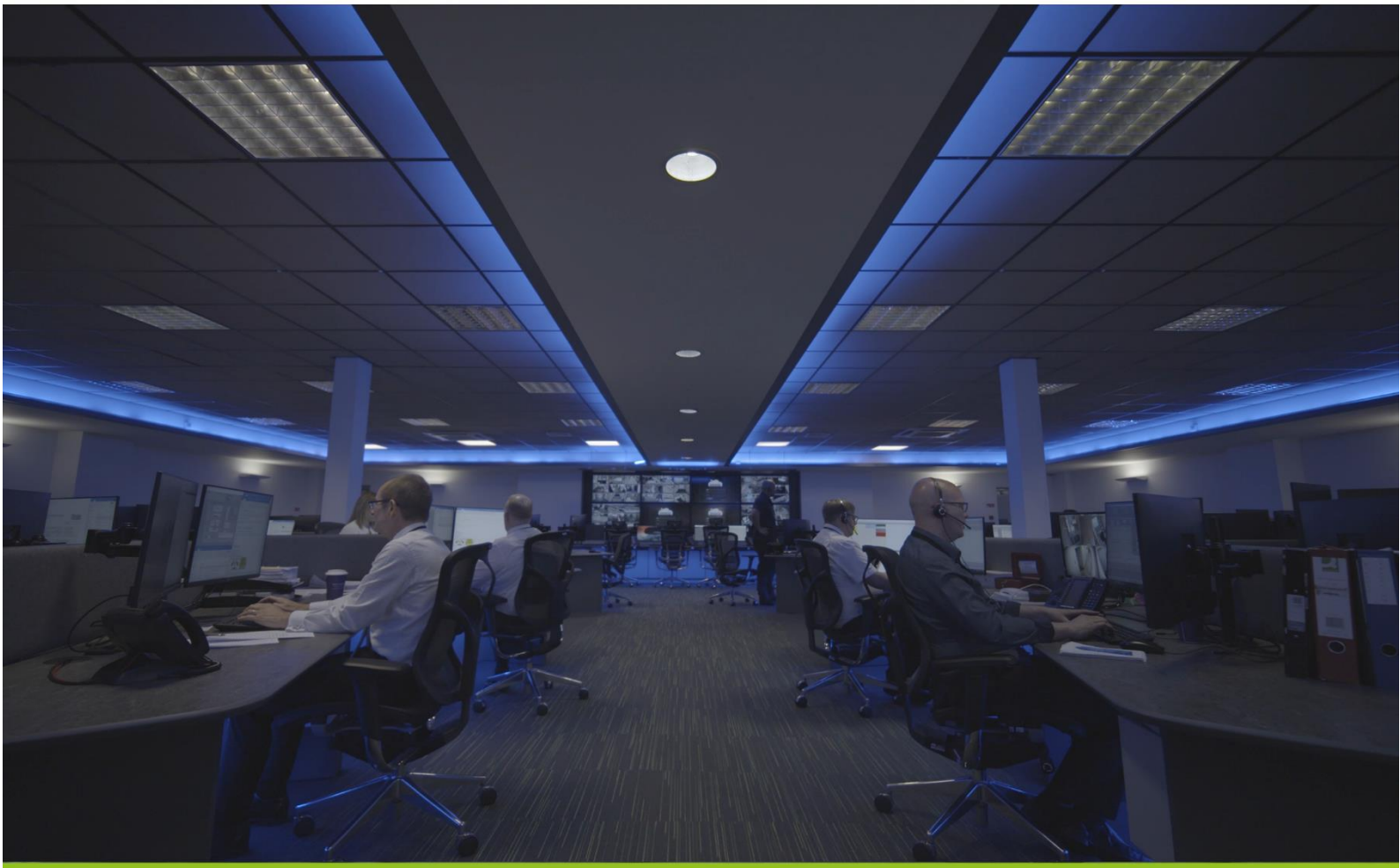
SMC
POWERED BY APi GROUP



# SMC UK&I Administrative and Operational Booklet

# Foreword

This booklet has been created to provide essential information regarding the services provided to Alarm Companies and End Users for the provision of both Alarm & CCTV monitoring services by SMC UK&I.

Split into two parts, the booklet now provides essential administrative & operations procedures set out for both SMC Custodian for alarm monitoring & SMC Vision for CCTV monitoring, where:

Part 1 of this document refers to SMC Custodian (Alarm Monitoring).

Part 2 of this document refers to SMC Vision (CCTV Monitoring).

# Part 1 - SMC Custodian

# Table of Contents


1. Introduction ..... 7

1.1 Scope ..... 7
1.2 Normative References ..... 7
1.3 Registration & Approvals ..... 8
1.4 Release Information ..... 8
1.5 Contact Details ..... 9

2. Technical Infrastructure ..... 10

2.1 Monitoring Structure, Disaster Recovery And Business Continuity ..... 10
2.2 Telecommunications (Voice And Data) ..... 10
2.3 Monitoring Product Approval ..... 10

3. ARC Administration ..... 11

3.1 ARC Administration Department ..... 11
3.2 Data Security (Passwords) ..... 11
3.3 Standard Forms ..... 11
3.4 Chips ..... 11
3.5 New Connections ..... 11
3.6 Transferring Systems To Our ARC ..... 11
3.7 Transferring Systems To An Alternative ARC ..... 12
3.8 Takeover Of Another Company's Monitored Connection At Our ARC ..... 13
3.9 Alarm Configuration ..... 13
3.10 Critical Data Omissions (CDO) ..... 14
3.11 Data Changes ..... 14
3.12 Monitoring Suspension & Reinstatement ..... 15
3.13 Cancellation ..... 15
3.14 Reports ..... 16

4. Commissioning Approved Monitoring Connections ..... 18

4.1 Monitoring Products ..... 18
4.2 Commissioning Procedure ..... 18
4.3 Commissioning Certification ..... 18

5. Alarm Monitoring Responses ..... 19

5.1 Alarm Response Performance ..... 19
5.2 General Requirements – Alarm Signal Processing ..... 19
5.3 Fire And Police (Agencies) ..... 19
5.4 Filtering Policy ..... 20
5.5 Mis-Operation Signals ..... 20
5.6 Fire Alarms ..... 20
5.7 Personal Attack/Hold-Up Alarm Conditions ..... 21
5.8 Intruder Alarms ..... 24
5.9 Types Of Confirmed Intruder Alarm ..... 25
5.10 Path Failure Alarm Conditions ..... 27
5.11 Fault And Other Advisory Alarm Conditions ..... 28
5.12 Linkdown Message ..... 30
5.13 Late Restoral Alarm Conditions (LRAC) ..... 30
5.14 Systems With Opening And Closing Time Schedules ..... 30
5.15 Digital Communicator – Timer Tests ..... 31
5.16 Unknown Signals ..... 31
5.17 Excessive Signals ..... 31
5.18 Calling Contacts/Keyholders ..... 31
5.19 Calling Premises ..... 32
5.20 Adverse Weather & Unforeseen Circumstances ..... 32

5.21 Mezzanine Services – Smart Response ..... 33
5.22 Multiple Signalling Sites/Systems ..... 33
5.23 Multiple Path Failures (Flood Conditions - Webway) ..... 34
5.24 Reasonable Alarm Monitoring And Associated Charges ..... 34
5.25 Omit/Re-Arm ..... 34
5.26 Pre ACPO Responses ..... 35
5.27 Suppression Of Sites Reporting Continuous Signals ..... 35

**6. Placing a System On or Off Test ..... 36**

6.1 Testing Conditions ..... 36
6.2 TOUCH For Engineers ..... 36
6.3 TOUCH For Customers ..... 36
6.4 On Test Expiry Conditions ..... 36

**7. Remote Restore (Remote Reset) ..... 37**

7.1 Remote Restore Procedures ..... 37
7.2 Registration ..... 37
7.3 Remote Restore By Company ..... 38
7.4 Remote Restore Flowchart ..... 38

**8. Company liability for accuracy of data held and system status at the ARC ..... 39**

8.1 Annual Audit ..... 39
8.2 Company Maintenance & Corrective Actions Visits ..... 39
8.3 Company Review And Action Of ARC Reports ..... 39

**9. Technical Information ..... 40**

9.1 Use Of Alternative Call Providers ..... 40
9.2 Twenty First Century Network And NGN's (Next Generation Networks) ..... 40
9.3 Using Contact ID/SIA To Overcome 21CN And NGN's Update ..... 40

**10. Product Support Software (Smart Suite) ..... 42**

10.1 Smartpac ..... 42
10.2 TOUCH (V1.0) ..... 42
10.3 Touchforms ..... 42
10.4 Touch (V2.0) ..... 42
10.5 Touch (V2.0) New User Authority Levels & Permissions ..... 43

**11. Additional Services ..... 44**

11.1 Out Of Hours Emergency Demand Service Calls ..... 44
11.2 Keyholder Care ..... 44
11.3 Lone Worker Monitoring Services ..... 46
11.4 Underwriters' Laboratories Of Canada (ULC) Requirements ..... 46

**12. Data Protection ..... 50**

12.1 General Data Protection Regulations (GDPR) ..... 50
12.2 Audio Recording For ARC Telephone Conversations ..... 50

**13. Cessation of Services ..... 53**

**14. ARC Suppliers ..... 53**

**15. Glossary ..... 54**

**16. Certification ..... 57**

**Part 2 - SMC VISION ..... 59**

**1. Introduction ..... 59**

**2. General Information ..... 60**

2.1 Police Response/Urns (Unique Reference Numbers) ..... 60
2.2 Alarm Company Security Codes ..... 60

2.3 End User Security Codes ..... 60
2.4 Connection Forms ..... 60
2.5 Instructing The Alarm Receiving Centre ..... 60

**3. CCTV Overview ..... 62**

3.1 Remotely Monitored CCTV Installations ..... 62
3.2 CCTV Surveillance System ..... 62
3.3 System Configuration ..... 62
3.4 Definitions And Abbreviations ..... 62
3.5 CCTV Monitoring ..... 63
3.6 Installation Standards ..... 63
3.7 CCTV Design Considerations ..... 64
3.8 Management Of CCTV Systems ..... 65
3.9 System Specification ..... 66
3.10 Monitoring Suspension & Reinstatement ..... 66

**4. CCTV Monitoring Contracts ..... 67**

4.1 Overview ..... 67
4.2 Responsibilities ..... 67
4.3 Contract Documents ..... 67

**5. Connection of CCTV Systems ..... 68**

5.1 How To Organise A Connection ..... 68
5.2 Preliminary Testing ..... 68
5.3 Making A System Live ..... 68

**6. Commissioning of Installations ..... 69**

6.1 Overview ..... 69
6.2 Commissioning Procedure ..... 69
6.3 Commissioning Requirements ..... 69
6.4 Acceptance Of System ..... 69

**7. Incident Handling Options ..... 70**

7.1 Overview ..... 70
7.2 Monitoring Options ..... 70

**8. CCTV Incident Monitoring ..... 72**

8.1 Active Incident Handling ..... 72
8.2 Response Plan ..... 72
8.3 Police Intervention ..... 72
8.4 Calling Contacts/Keyholders ..... 73
8.5 AI Analytic Alarm Filtering ..... 73
8.6 Proactive CCTV Maintenance Check ..... 73

**9. False Alarms ..... 74**

9.1 General ..... 74
9.2 Multiple False Alarms ..... 74
9.3 Disablement Procedure ..... 74
9.4 Testing Conditions ..... 75

**10. Remote Access to Site ..... 76**

10.1 Preventative Maintenance ..... 76
10.2 Corrective Maintenance ..... 76
10.3 Walk Testing ..... 76

**11. Records and Reports ..... 77**

11.1 Overview ..... 77
11.2 Detail Of Records ..... 77
11.3 Reports ..... 77

12. Quality Checks ..... 78
12.1 Weekly System Health Checks ..... 78
12.2 Live Incident Quality Checks ..... 78
12.3 Critical Data Omissions ..... 78
13. Service Levels ..... 79
13.1 Incident Response Time ..... 79
13.2 Local System Fault Reporting ..... 79
13.3 Telephone Response ..... 79
13.4 Incident Investigation ..... 79
13.5 Customer Complaints ..... 79
13.6 Event Reporting ..... 80
13.7 New Site Connection ..... 80
13.8 Adverse Weather & Unforeseen Circumstances ..... 80
14. Data Protection ..... 81
15. Video Verified Systems ..... 81
16. Cessation of Services ..... 81
Appendix A – SMC Privacy Notice ("Notice") ..... 82
Appendix B – Operator Assist Process ..... 85
Appendix C – Typical CCTV System Policy Statement ..... 86
Appendix D – Surveillance Camera Code of Practice – 12 guiding principles ..... 88
Appendix E – SMC Telephone Call Flowcharts ..... 89
Appendix F – Summary of Key changes to this document (Issue 31.0) ..... 93

# 1. Introduction

## 1.1 Scope

This booklet and the material recorded herein is the property of Security Monitoring Centres UK&I trading as SMC Custodian and shall not be used or copied without our express permission. Companies who connect monitored services with us are entitled to use extracts from this document to form their own terms and conditions of service to their customers.

This booklet sets out essential information regarding the administrative and operational services provided to Companies and End Users for the provision of monitoring services and should be read in conjunction with our standard terms and conditions. Although we have attempted to cover all aspects of service provision, the references cannot be exhaustive, and our trained staff are always available to assist you further.

Prior to connecting systems to our ARC, you will need to have agreed a monitoring contract with us. Should a contract not be in place please contact our sales hub.

Alarm Responses stated throughout this booklet are in accordance with the NPCC Policy, ACPOS Policy and the industry standards noted under “Normative References” below. Reference to pre-ACPO 2000 Alarm Response Plans and Alarm Response Plans for Alarm Systems that do not incorporate Alarm Confirmation are stated within section 5.26.

Throughout this booklet “Company” refers to the organisation that provides service and maintenance for alarm systems or who pays for the monitoring service for example Alarm Company, National Account or End User, see Glossary for further definitions and abbreviations used throughout this booklet.

Our commitment to the continual improvement of our quality systems and procedures to meet the needs of our clients and to reflect changes in industry requirements means the contents of this document are subject to change without notice.

## 1.2 Normative References

This booklet has been formulated from Industry Standards and is intended as a guide to Companies who connect monitored services with our Alarm Receiving Centre (ARC). This guide is based on, and should be read in conjunction with, the following reference documents:

- ACPO (Association of Chief Police Officers) Security Systems Policy
- NPCC (National Police Chiefs Council) Security Systems Policy
- Police Scotland - Security Systems Policy
- BS5839 Fire detection and alarm systems for buildings
- BS8473 Code of practice for management of false alarms
- BS5979 Code of practice for remote centres receiving signals for security systems
- BS7858 Code of practice for security screening of individuals employed in a security environment
- BS8418 Code of practice for the installation and remote monitoring of detector activated CCTV systems
- BS8484 Code of practice for the provision of lone worker device (LWD) services
- BS8243 Code of practice for the Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions
- BS9518 Processing of alarm signals by an alarm receiving centre Code of practice
- BS EN 50131-1 Alarm systems - Intrusion systems - Part 1. General requirements
- BS EN 50131-6 Alarm systems - Intrusion systems - Part 6. Power Supplies requirements
- BS EN 50136 (All parts), Alarm Systems - Alarm transmission systems and equipment
- BS EN 50518 Monitoring and Alarm Receiving Centre
- PD6662 Scheme for the application of European standards for intruder alarm systems
- Data Protection Act
- General Data Protection Regulation (GDPR)

For alarm systems installed in Southern Ireland the following documents are also referenced:

- IS228 Monitoring Centres for Intruder Alarm System
- SR25 ARC Alarm Handling Procedures
- SR41 Electronic Security Services – Monitoring Services

- Garda Siochana Policy on Monitored Intruder Alarms
- PSA 33 Licensing Requirements for CCTV Monitoring and Alarm Monitoring Centres

For alarm systems installed in Canada the following documents are also referenced:

- CAN/ULC-301 Standard for Signal Receiving Centres Configurations & Operations
- CAN/ULC-561 Standard for Installation & Services for Fire Signal Receiving Centre & Systems

Installing and maintenance companies should also ensure that the technical requirements of control panel manufacturers and monitoring transmission providers are complied with.

### 1.3 Registration & Approvals

Our Alarm Receiving Centres operate as trading divisions of Security Monitoring Centres Limited, registered in England No. 318215.

Our Alarm Receiving Centre (ARC) is assessed under the National Security Inspectorate (NSI) Gold Scheme as a Category II ARC for the monitoring of Fire and Intruder Alarms, additionally:

- Our Nottingham ARC is registered with the Private Security Authority in Ireland for the monitoring of Intruder Alarms and CCTV Alarm Systems. We hold approval through CerticCS for the monitoring of Intruder Alarms in the Republic of Ireland. We are assessed by the NSI for the monitoring of Lone Worker Devices, detector activated, and other CCTV systems used in security applications.

Our Nottingham ARC is further assessed by the Underwriters Laboratories of Canada (ULC) for the monitoring of Fire and Intruder Alarms in accordance with the requirements set out in CAN/ULC-S561 & S301.

For further details refer to the certificates of approval within section 16.

We operate under the strict guidelines for ethics, service quality, protection of the environment and protection of health & safety of our parent company and our Health & Safety Management System is registered with CHAS.

### 1.4 Release Information

Issue 31.0 of this document replaces the previous issue 30.2 of June 2023

Please refer to Appendix F for details of key changes made to this issue.

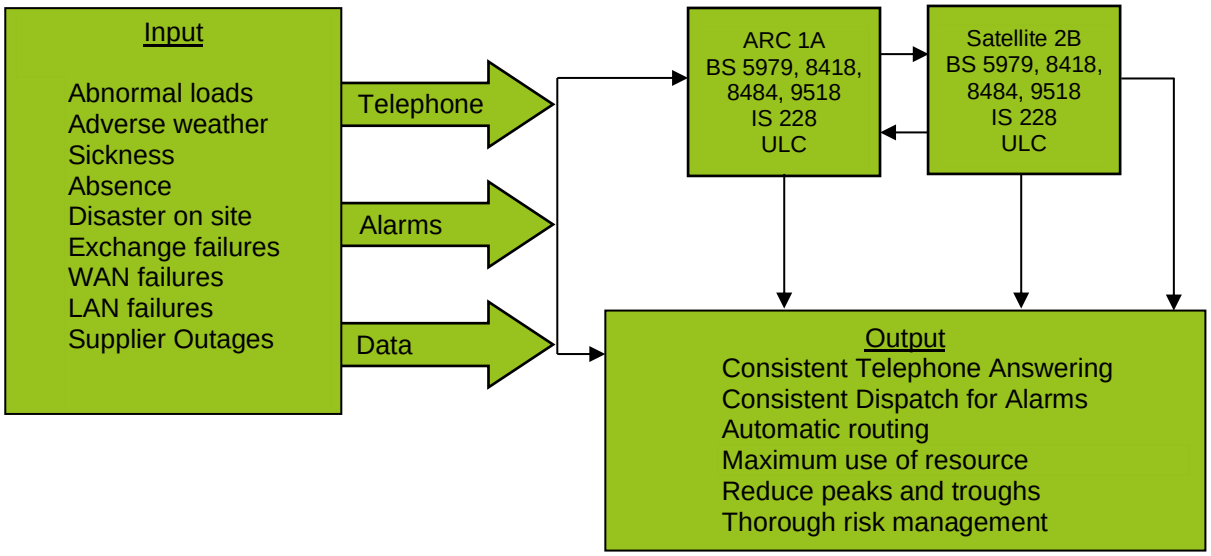
### 1.5 Contact Details

| **Sales** (Mon – Fri 08:30-17:00) | |
|---|---|
| Monitoring<br>Tel: 0844 879 1702 Opt. 1<br>Email: uk_sales@smc-monitoring.com | SMC Vision (CCTV)<br>Tel: 0844 879 1007 |
| **ARC Nottingham** (24/7) | **SMC Vision Nottingham** (24/7) |
| Crocus Street<br>The Meadows<br>Nottingham<br>NG2 3EJ<br><br>Operations: 0844 879 1703<br>Email: csm-nott@smc-monitoring.com | Crocus Street<br>The Meadows<br>Nottingham<br>NG2 3EJ<br><br>Tel: 0844 879 1911<br>Email: rvr@smc-monitoring.com |
| **ARC Administration UK only** (Mon – Fri 08:30-17:00) | |
| Tel: 0844 879 1704<br>Email: Orders (UK only): orders@smc-monitoring.com<br>Email: For Schedules: schedule@smc-monitoring.com<br>Email: For URN's: urn@smc-monitoring.com<br>Email: Cancellations: cancellations@smc-monitoring.com<br>Email: Data Changes: data-changes@smc-monitoring.com<br>Email: SMC Vision Admin: Uk_rvradmin@smc-monitoring.com | |
| **SmartPAC & TOUCH** (Mon – Fri 08:30-17:00) | |
| Touch v1.0 & SmartPAC: www.smc-monitoring.com<br>Touch v2.0: Touch v2.0 - Login<br>Touch v2.0 Registration: smc-touch.co.uk/registration<br>Touch Helpdesk: touch.estate@smc-monitoring.com | |
| **Head Office** (Mon – Fri 08:30-17:00) | |
| Security Monitoring Centres Limited<br>Crocus Street<br>The Meadows<br>Nottingham<br>NG2 3EJ<br><br>Tel: 0844 879 1701<br><br>Credit Control: 0800 028 3082<br>Email: UK_collections.cmrs.uk@smc-monitoring.com | |

# 2. Technical Infrastructure

### 2.1 Monitoring Structure, Disaster Recovery and Business Continuity

Through significant investment, our ARC is supported via a redundant network to which enhanced alarm and voice call routing is managed. To best optimise service delivery, companies are normally supported by a 'host' centre within our group. However, we may provide services from an alternate centre to maintain customer service levels.




The above network supports our disaster recovery and business continuity plans. All our processes are checked based on their impact and probability of occurrence and we endeavour, where possible, to ensure all high risk areas are replicated to minimise the risk of service failure.

### 2.2 Telecommunications (voice and data)

To support disaster recovery and business continuity our ARC uses non-geographic services (08/09 numbers) across the business. Companies and End Users need to ensure that both voice and machine to machine alarm services can connect to these networks and that these numbers are not barred for any reason.

The use of DDI (Direct Dial Inwards) numbers to contact the ARC is not recommended and will not form any part of the ARC disaster recovery and business continuity plans. Our ARC will not accept any liability for Companies or End Users using DDI numbers.

To aid customer identification our ARC operates a screen popping service whereby the premises are automatically identified to the ARC Agent if an inbound telephone call sends 'Caller Line Identification' and the telephone number is within our monitoring database.

All telephone calls are recorded as required by BS5979.

**Our primary telephone service utilises 0844 prefix telephone numbers, telephone calls provided by BT will be charged at up to seven pence per minute. An access charge may also be levied by your telecoms carrier, mobile costs may vary. (This statement is correct at the release date of this document).**

### 2.3 Monitoring Product Approval

In the event a supplier wishes to bring a new product to the monitoring market, we have a multiple staged approval process to ensure the product is compatible with our monitoring network and that we have configured response plans to interpret alarm signals received.

Companies using equipment connected to our ARC that have not been approved, do so at their own risk. The full list of currently approved monitoring products are detailed in our monitoring application forms.

# 3. ARC Administration

### 3.1 ARC Administration Department
Our ARC administration is provided by a dedicated centralised team, including a helpdesk for non-operational enquiries. In emergencies, our operational centres can support basic administrative functions but we ask that wherever possible these are requested during normal office hours only (Mon–Fri 08.30 – 17.00).

### 3.2 Data Security (Passwords)
All ARC operates a security discipline that requires persons contacting the ARC by telephone to have a valid password before security information can be exchanged. In general, verbal enquiries will be significantly enhanced in speed and accuracy if the persons calling are also able to provide the ARC's 'system' reference number.

An audit of engineer's and customer authorised access provision should be completed by the Company at least once per annum. If a customer or engineer is no longer an employee of the Company or End User Site, the ARC should be notified immediately so their details can be terminated from the ARC monitoring system.

### 3.3 Standard Forms
Due to the security nature of instructions and to provide consistency and minimise errors it is preferred that all applications for monitoring, subsequent data changes and cancellations are submitted electronically via our standard TouchForms which are available to authorised Service Companies via TOUCH or SmartPac click on these links or to our website, https://smc-monitoring.com/ for further details.

Please refer to the relevant sections for expected processing timescales.

### 3.4 Chips
As BT have announced that the Public Switch Telephone Network (PSTN) will close in January 2027, meaning by then every phone line in the UK will have moved to a fully digital network that uses Internet Protocol (IP) across a fibre-based service, all requests for programmed chips will now be individually reviewed and those considered necessary may incur a processing charge of £30 + VAT per chip.

All accepted requests for programmed chips should be made by completing the appropriate section of the monitoring application form or a separate chip order form. It is important that you do not assume we are familiar with your programming requirements. Please state clearly on each application the polarity, type and any special requirements.

Chips are normally supplied to the address of the Alarm Company only. The ARC cannot guarantee delivery dates where obsolete or non-standard chips are requested.

### 3.5 New Connections
All new connections submitted by TouchForms will be automatically delivered.

Any Non-Form orders should be submitted to orders@smc-monitoring.com

On a normal working day we will aim to process each new order within 1 working day of receipt. The normal working day is defined as: 0830 - 1700, Monday to Friday excluding 'English' bank holidays. Please note that product delivery is determined by the supplier and may be impacted by external influences.

Please note, UPG orders are subject to a minimum 7 days order processing time and for larger UPG orders this may be a minimum of 10 days.

### 3.6 Transferring Systems to our ARC
#### 3.6.1 Single Transfer-in
Ensure that our ARC Administration is in receipt of an appropriately completed TouchForm (Application Form).

The Application Form must be completed in full as these are not provided via the transfer process and or the losing ARC.

Once the service provider has received the losing ARC's acceptance, the transfer can go ahead. Our ARC will then inform you that the system is ready and an engineer may be required to attend site and complete the transfer.

The engineer should ensure:

- The system is put on test and they advise us they are transferring the monitoring service from another ARC to us. (Wherever possible our helpdesk will contact the service provider to move the service to our centre but circumstances may require us to call the engineer back).
- Every channel is activated noting order of transmission, i.e. Intruder, Open, Close, Restore, etc.
- The requirements of Section 4.0, Commissioning Approved Products, are followed.
- We have received the correct channels in the appropriate order and have all the correct data, e.g. Contacts/Keyholders, etc.

The system will normally be made 'LIVE' following expiry of the initial test period unless we are instructed otherwise by the engineer.

### 3.6.2 Volume Transfer-in

The Company is required to provide full details of each connection to be transferred in, including:

- Site Names & Addresses
- Contact Details
- URN's and their status
- Zone Details & Response Plans (including any reverse signalling)
- Open/Close Details & Schedules where required (including any reverse signalling)
- System/Signalling Numbers (E.g., STU / TA Number)
- Remote Resets
- Data/SIM numbers (Where applicable)

ARC Administration will add the details to the Monitoring System Database.

Once agreement is reached that all system details are correct a date of transfer can be agreed between the Company, the monitoring service provider and both ARC's.

ARC Administration on the day of transfer and following days as required will undertake a series of signalling audits to best ensure that the systems transferred are signalling correctly or alternatively any specific commissioning requirements agreed with the Company are carried out.

## 3.7 Transferring Systems to an alternative ARC

### 3.7.1 Volume Transfer-Out

The ARC's agreement to participate in the transfer of monitored systems to another ARC, unconnected with us, is dependent on the existing contractual arrangements in place between the Company and our ARC. Terms and conditions can apply to both the Company's overall account and to individual monitored systems i.e.

- The account is within an initial fixed term.
- A particular monitored system was ordered as part of a promotion that has a fixed term.
- The monitored system is within its first year.

The agreement to transfer or the agreement to a date of transfer will also be dependent on the payment of any outstanding or future invoices.

Outside of the above criteria the following process will be followed,

1. A written instruction is required from the installer authorising our ARC to provide information to them.
2. The alternative ARC and/or supplier, on the Company's behalf, shall provide our ARC with a list of systems requiring transfer. Once agreement is reached that all system details are correct, a date of transfer can be agreed between the Service Provider and both ARC's.
3. On completion of transfer to your new ARC it is the installers responsibility to advise us of all sites which have transferred successfully that required cancellation. Any system that could not be transferred, it is the installers responsibility to advise when transfers are complete.

SMC accept no liability or financial loss for sites transferred which you have not notified us to cancel.

All rights and liabilities placed on our ARC shall cease at the time of transfer.

### 3.7.2 Single Transfer-Out

The ARC's agreement to participate in the transfer of monitored systems to another ARC, unconnected with us, is dependent on the existing contractual arrangements in place between the Company and our ARC. Terms and conditions can apply to both the Company's overall account and to individual monitored systems, i.e:

- The account is within an initial fixed term.
- A particular monitored system was ordered as part of a promotion that has a fixed term.
- The monitored system is within its first year.
- The agreement to transfer or the agreement to a date of transfer will also be dependent on the payment of any outstanding or future invoices.

Outside of the above criteria the following process will be followed,

Upon receipt of a Transfer out request (Form) we will seek to ensure the correct site is being referred and that there are no contractual obligations to be observed.

Our ARC Administration will submit losing instruction to whichever supplier is involved and will confirm by email to the company transfer is ready.

After 7 days ARC Administration will validate the transfer was completed and will cease our services however, if signalling remains with our ARC we will retract the transfer request in full and inform the company to re-submit.

### 3.8 Takeover of another Company's Monitored Connection at our ARC

It is imperative that the following procedures are adhered to at all times.

1. Both companies involved with the takeover must write to the ARC stating their intention to either release or to accept the end-user to their account. Note: without these documents the ARC will not be able to transfer the site as it is contracted to the current Company. Companies can use the standard application forms.
2. The instruction to release should also include a clear agreement to release both the signalling services and the data held for the system.
   If the instruction only releases the signalling, the takeover company will need to supply all data as per a new application.
3. All critical data should be reviewed with the end-user to ensure accuracy.
4. The Company should check the ARC responses are correct and will meet the end-user expectation, attention should be given to pre and post ACPO 2000 responses.
5. Transfers should be carried out Monday to Friday 09-00hrs to 17-00hrs, excluding all bank holidays.
6. Billing will continue up to the transfer date and the out-going Company will be responsible for these charges. After the transfer the new company will be responsible for any transfer costs and the on-going monitoring charges.
7. The gaining company may need to notify the Police authority, (using Appendix "F" of the Police Force Policy), prior to the transfer informing them of the transfer. This may include a fee dependant on the authority. Failure to notify the authority prior to the transfer may render the URN null and void.
8. When the transfer is complete the ARC will normally confirm the cancellation to the outgoing company and a new connection to the new company.
9. It is strongly recommended the system is re-commissioned and fully tested to our ARC as detailed in section 4.2.
10. In the event the out-going company will not release an end-user account to a new provider the only option is for the new provider to apply for a new account in the normal way.
11. The ARC will not accept any responsibility if these procedures are not adhered to in full.

### 3.9 Alarm Configuration

To establish a common approach across the ARC, the default communication channel designations are detailed in the commissioning section. TouchForms will normally default by system type to these zones with the appropriate agreed business response. If you wish to deviate from these standard responses this must be clearly indicated on your application or through a pre-existing agreement of default responses.

### 3.9.1 Changing grade of monitoring products

In the event the monitoring service is re-graded it is essential that the following guidelines are adhered to:

1. The customer should be notified and the alarm system specification updated.
2. It is recommended that the customer is advised to obtain agreement from their insurance company of the grade change.
3. When transferring the data from the old product to the new product a full commissioning test should be carried out, see section 4.2.

The ARC does not accept any liability for changes in monitoring product, unless items one; two and three above are completed in full.

### 3.9.2 Pre-ACPO 2000

Should an existing system be transferred to us and a pre-ACPO 2000 alarm response is to be retained, we must be clearly instructed of this requirement on the application form.

### 3.9.3 Channel Configuration for EN50131 Systems

Under EN50131 & PD6662 there are requirements to send additional signals such as AC Mains Fail and Tamper faults to the ARC. The main additional requirements are dependent on System Grade as follows:

- For Grade 3 and Grade 4 systems, it is necessary to send AC mains fail signals if the standby battery capacity is to be halved from 24 hours to 12 hours
- For Grade 3 and Grade 4 systems, it is necessary to send tamper signals to the ARC in the set and unset conditions

### 3.10 Critical Data Omissions (CDO)

In the event that any critical information is missing on completion of a connection, (e.g., Contacts/Keyholders, telephone numbers, URN's, etc.), the Company will be informed of missing information, usually by e-mail. There is also a CDO report which can be run via SmartPAC.

Failure to run or act upon reports received and make corrective actions could result in customers/end-users not receiving the correct alarm dispatch, information they have paid for or incurring additional cost. Our ARC will not accept any liability for failed alarm dispatch or telecommunications costs from a third-party supplier or customers/end-users where reports have not been addressed with appropriate corrective actions.

### 3.11 Data Changes

Please note data changes should be facilitated using your TOUCH portal as this is available 24/7. Any changes made are effective without delay.

### 3.11.1 Custodian processed changes

All data changes should be completed on TouchForms. On a normal working day we will aim to process all data change requests within two working days from receipt, however this can be affected by public holidays and external factors which may increase volumes received.

Please send any requests at your earliest opportunity to ensure they can be processed efficiently. The normal working day is defined as: 0830 - 1700, Monday to Friday excluding 'English' bank holidays. Please ensure that all requests contain all relevant detail, including CS / Contract number and clear instructions on what is required to avoid any unnecessary delays.

All requested amendments must be submitted via the documented ARC Administration contact details listed in section 1.5. SMC UK&I accepts no liability should any requests be submitted via alternative channels not listed in the ARC Administration contact details listed in section 1.5.

Emergency changes relating to Contacts/Keyholders, passwords, site and contact telephone numbers or open/closing times, can be accepted directly from end users, provided they are registered Contacts/Keyholders and hold legitimate passwords**.** We reserve the right to raise an additional charge for non-standard or bulk requests for changes.

### 3.11.2 Company processed changes

Amendments to the ARC database via SmartPAC or TOUCH by the company or authorised user should be audited by the Company to ensure the changes are correct. Our ARC accepts no liability for changes made incorrectly causing an error in alarm dispatch or alarm reporting.

For further information and assistance contact our administration team on telephone 0844 879 1704

For technical related support, please contact our SmartPAC help desk on telephone 0844 879 1712 or email: smartpachelpdesk@smc-monitoring.com or touch.estate@smc-monitoring.com

### 3.11.3 Contacts/Keyholders

All change requests should list 'all Contacts/Keyholders', this will enable us to check that we have them listed in the correct sequence and update our records accordingly. For changes made via SmartPAC or TOUCH it is important that all Contacts/Keyholders on the database have a sequence number and contact telephone number, Contacts/Keyholders with no sequence or telephone numbers will not be presented to an ARC operator for alarm dispatch.

For SmartPAC users the "Contact Type" should be set to "M" and the "Relation" and "Authority" set to "Key".

If during the processing of an alarm we are advised that a person is no longer a Contact/Keyholder we will normally insert an end date against their record and create a CDO informing the company of this change. This is to avoid multiple contact with people who insist they are no longer Contacts/Keyholders.

### 3.11.4 Police and Fire Authority URN's

It is important when advising the ARC of new or changes to existing Police and Fire Authority URN's that the elements the URN applies to be specified i.e.

- PA only
- INTRUDER only
- PA & INTRUDER
- Fire only

It is also important to ensure which Police or Fire Authority is applicable.

## 3.12 Monitoring Suspension & Reinstatement

### 3.12.1 Suspension

A method used by the ARC to ignore all alarm conditions for a period of more than 24 hours. All instructions must be confirmed in writing or via TouchForms:

- Billing will continue during the suspension period.
- The ARC will not allow suspensions with an end date.
- The Company must review the suspended systems weekly to ensure the suspension is still required.

### 3.12.2 Re-instatement

The instruction to reinstate a suspended system is normally required in writing but may be accepted over the telephone from an Authorised Contact/Keyholder, Company Representative or Engineer.

## 3.13 Cancellation

To ensure the accurate and timely cancellation of monitoring services, requests to cancel will only be accepted by the completion of the appropriate TouchForm, Company Email or Letterhead to the Administration Department by one of the following options.

- Form submitted by TouchForms will be automatically delivered.
- Email: cancellations@smc-monitoring.com

IMPORTANT:

1. Cancellations may take up to 5 working days from receipt to process to allow time for verification and approval where necessary, subject to contract.
2. We will not respond to alarm signals received following cancellation and it is important that the communicator at the protected premises is removed or disabled to prevent further signals being transmitted and associated telephone charges being incurred.
3. Please note cancellation requests will only be accepted from the contract holder in line with their Terms & Conditions.

### 3.14 Reports

#### 3.14.1 Business Critical Daily / Weekly Reports

Our ARC provides the following reports via SmartPAC or TOUCH. It is strongly recommended that all these reports should be run daily / weekly and corrective actions completed on a daily / weekly basis.

1. **Daily Activation Reports History** – Lists all alarm incidents in the specified date range
   (Reports / History / Activations - Incidents / Activations-Incidents – with actions / Compact)
2. **Sites not Connected** – Lists sites ordered but not connected OOS (out of service) category "NEW"
   (Reports / Client / Pending Connections)
3. **Systems in Path Failure** – List all sites in path failure
   (Reports / Management / Unrestored Alarms / NR- Line Faults)
4. **High Activity Sites** – Lists the top twenty most active sites
   (Reports / History / Top 20 Most Active Systems)
5. **New Connected Sites Reports** – Lists the newly connected sites for the date range specified
   (Reports / Client / Newly Connected Sites)
6. **Systems in Alarm Condition** – Lists Unrestored alarm conditions
   (Reports / Management / Unrestored Alarms – NR's and LF's)
7. **False Alarm Management** – List all alarm conditions that require a reason code
   (False Alarm Management / Quick Resolve / Reasons for policeable Incidents)
8. **Suspended Systems –** the status on the right indicates on-line (live) or suspended
   (Reports / Client / Site Summary)

#### 3.14.2 Company Business Critical Monthly Reports

Our ARC provides the following reports via SmartPAC or TOUCH. It is strongly recommended that all these reports are run monthly and corrective actions completed.

1. **Systems with No URN and URN Status** – Lists URN status
   (Reports / Client / Police URN / No Police URN or URN status)
2. **Change of Details** – List sites that have changed data in the range specified
   (Reports / Client / Changed Client / Client Changes / Summary or Detail)
3. **False Alarm Management** – Lists the BS8473 Form
   (False Alarm Management / FAM Model Form / Policeable Incidents)

   The SmartPAC reports suite allows companies to assign disposition codes against alarms and as an aid to compliance with BS 8473 Intruder and hold-up alarm systems – Management of false alarms – Code of practice.

   Our ARC encourages the management of false alarms and strongly recommends the use of the specific software written by the ARC to highlight reasons why alarm systems create false alarms and corrective actions to reduce false alarm signal traffic to the ARC.

   Reports available via SmartPAC or TOUCH are:

   **1 - Quick Resolve Report**
   Using the quick resolve report, you can enter dispositions / reasons for the alarm activity quickly. Note reasons are required for both policed and non-policed events.

   **2 - Disposition Reasons Summary Report**
   If you run this report, you can breakdown the categories to see the detail of your dispositions (reasons).

   **3 - BS 8473 Report**
   Report of signalled/notified alarm conditions

It is the Company's responsibility to ensure that reports detailed in sections 3.10 (Critical Data Omissions) & in this section whether available via SmartPAC Reports or as received directly from the ARC are reviewed to identify and amend any missing or incorrect data. Failure to do this could result in customers/end-users not receiving the correct alarm dispatch, information they have paid for or incurring additional cost. Our ARC will not accept any liability for failed alarm dispatch or telecommunications costs from a third-party supplier or customers/end-users where reports have not been addressed with appropriate corrective actions.

#### 3.14.3 Automated Reports

The following automated reports are available to the Company on request:

1. **Daily Activation Reports History** – Lists all alarm incidents in the specified date range

(Reports / History / Activations - Incidents / Activations-Incidents – with actions / Compact)

2. **Systems in Path Failure** – List all sites in path failure
   (Reports / Management / Unrestored Alarms / NR- Line Faults)
3. **High Activity Sites** – Lists the top twenty most active sites
   (Reports / History / Top 20 Most Active Systems)
4. **Health Check Report –** this includes:
   - Systems Awaiting Connection
   - New Systems within the last 12 months
   - Suspended Systems
   - Systems Cancelled within the last 12 months
   - Systems with No Site Password or Common Key-Holder Password
   - Systems with less than 2 Key-Holders
   - Systems Missing Data such as Premises Phone or Postcode
   - Systems without an Agency or URN
   - Systems with Reduced Police Response
   - Systems with No Scheduled or Log-Only Open/Close within the last 30 days
   - Systems with Unrestored Zones
   - Systems with greater than 5 activations within the last 12 months
   - Systems Out of Service
   - Systems with Keyholding Company
   - Fire System with No Fire Brigade Response
   - Systems with a Policeable Event but no URN
   - System with a valid URN but No Policeable event

5. **Service Call Report (out of hours engineer call handling)**

# 4. Commissioning Approved Monitoring Connections

### 4.1 Monitoring Products

Our ARC's support all major suppliers and their associated products in the security industry. Any new products go through our product approval process, referred to in section 2.3, before being connected to our ARC network.

Every new connection and system upgrade should always be commissioned to our ARC network as detailed below.

### 4.2 Commissioning procedure

The following procedure must be adopted for all new, transferred and system upgrades.

1. Submit an approved application form to ARC Administration at least 24hrs in advance.
2. Ensure the Commissioning procedure can be completed during normal working hours and before 16:00 hours if possible.
3. Contact our Administration Help Desk via 0844 879 1704 (Not ARC Operations or SmartTEST).
4. Confirm what services are being connected and request the system to be placed 'in-service' & 'on-test'.
5. Test each alarm & restore condition, including single and dual path failures.
6. Check all the ARC responses meet with the end-users expectations.
7. Panel manufacturers and signalling providers may delay certain types of alarm conditions to the ARC so be aware of these delays and how they can be tested.
8. Contact our Administration Help Desk via 0844 879 1704 (Not ARC Operations or SmartTEST) for test results.
9. Confirm all alarm signals sent have been received in the correct order.
10. The Help Desk will validate the 'Signalling Test' and ensure that all the information required to support the Alarm Response has been provided.
11. On completion, the site will be taken off test and a commissioning report submitted to the Company.

Note:

1. Where there is an urgent need to connect a new monitored system out of normal business hours our ARC Operations Team Leaders are available to assist.
2. If you are registered for Touch v2 and the below criteria are met, commissioning can be completed using the included commissioning tool.
3. SMC accepts no liability for any systems that are commissioned incorrectly using Touch v2.0 as a result of incorrect data entry, usage or set up by the installer.

### 4.3 Commissioning Certification

To help the Company identify that the alarm system is commissioned to the ARC, two critical elements for effective monitoring are assessed during the commissioning process before being passed in line with relevant Standards.

1. **Signalling** – All zones and path failures including dual path failures have been tested and the engineer has called back after the test to validate the results.
2. **Data** - All Critical Data is present on the monitoring system (MAS), for example:
   Name
   Address & Post Code
   Premises Tel Number
   Keyholders – Minimum of 2 with appropriate contact numbers (or 1 if a Keyholding company)
   Password for authentication of false alarms & other enquiries

Please note that systems commissioned using Touch are assessed using the same criteria outlined above

# 5. Alarm Monitoring Responses

### 5.1 Alarm Response Performance

Our ARC undertakes to meet the standards for contacting the emergency services as set out in BS5979 for Category II ARC's, which are:

1. Fire 30 seconds for 80% & 60 seconds for 98.5% signals received
2. PA 30 seconds for 80% & 60 seconds for 98.5% signals received
3. Intruder 90 seconds for 80% of signals received and 180 seconds for 98.5% of signals received

These targets are exclusive of any imposed filtering period and exceptional circumstances such as extreme weather conditions and the associated abort signals received under these conditions.

Alarm processing may be dispatched via an immediate automated notification method, i.e., text*, email, telephone.

### 5.2 General Requirements – Alarm Signal Processing

Our standard response to alarm signals is detailed within this section. All actions taken by the ARC are as indicated unless the Company advises otherwise. It is the responsibility of the Company to advise the End User what action the ARC will normally follow on receipt of an alarm signal.

All alarms are assigned a priority as indicated in the table below. In the event of multiple alarm signals only the highest priority alarm will be processed.

| Item | Priority |
|---|---|
| Fire | 1 |
| PA | 2 |
| Confirmed Intruder | 3 |
| Intruder | 4 |
| Comms Fault | 5 |
| Trouble | 6 |
| Environmental | 7 |

Our ARC will only act on alarm signals received at the ARC. The CIE should recognise combinations of alarm types as valid for generation of confirmed intruder/hold up alarms. SMC accept no liability for signals lost for whatever reason by suppliers or their agents.

### 5.3 Fire and Police (Agencies)

Agencies may have individual policies which you must comply with to ensure we can dispatch alarms to them on your behalf. The ARC has dedicated telephone numbers with most agencies where appropriate. ECHO (Electronic Call Handling Operation) is approved and utilised in conjunction with the NPCC. Full details of associated forces can be found at www.echo.uk.net.
Agencies will respond in accordance with their published policies and where they require a URN, it is the responsibility of the Company to ensure the ARC is in possession of a valid URN and its response status is 'active'.

Our ARC will not be liable for delays in response from agencies.

It should be noted that within any contractual agreement or communication we cannot make any commitment that would involve assuming the powers of a civil authority, i.e., UK Police, Garda Siochana or Fire Service, etc.

In some cases, agencies may request the Company or the ARC to deviate from normal policy. In these circumstances requests should made in writing from the agency and directed to the Customer Service Manager or the National Administration Manager. On receipt we will propose a solution and communicate with the company. Such variations should be kept to an absolute minimum. The ARC does not accept any liability for procedures that deviate from standard policy.

Current policies can be accessed from the following web sites. Note these may have regional variances.

**NPCC policy (England and Wales)** - http://www.npcc.police.uk/
England, Wales and Northern Ireland Police Response to Security Systems

**Police Scotland -** http://www.scotland.police.uk/
Scotland Security Systems Police Policy

**CFOA policy -** nationalfirechiefs.org.uk
Fire Authorities Policy

### 5.4 Filtering Policy

The following filtering techniques are in accordance with NPCC Policy, Police Scotland Policy, BS8243 and BS5979.

For alarm systems installed in Southern Ireland the filtering requirements of 'Monitoring Centres for Intruder Alarm Systems' (IS228) and the Garda Siochana Policy on Monitored Intruder Alarms apply.

### 5.5 Mis-Operation Signals

All systems shall either:

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

or

2. Be capable of generating a secondary signal to indicate that the alarm system has been mis-operated.

Where we are unable to identify whether the system is set/unset (open/closed) we will action as "closed".

All intruder alarm conditions are delayed in accordance with the relevant agency policy waiting for a mis-operation signal to abort the alarm. These are:

1. Open
2. Abort

At any time if the ARC receives items 1 or 2 the alarm condition will be automatically aborted due to mis-operation.

#### 5.5.1 Open/Close with monitored line communications

Where the ARC is asked to monitor communication path failures, i.e., PSTN/GPRS/GSM/IP Networks & others it is imperative that the transmission equipment is programmed to send open/close signalling to the ARC without exception. The reason for open/close is to allow the ARC to make decisions based on the status of the alarm system to conform to NPCC and EN50131. Failure to enable open/close signalling may render an incorrect response to alarm conditions received at the ARC.

### 5.6 Fire Alarms

| Type of Alarm | Action taken by our ARC |
|---|---|
| Fire Alarm none (CFOA) region | Fire Brigade & Contacts (101) |
| Fire Alarm (CFOA) region | Premises, Fire brigade & Contacts (123CF) |
| Fire Alarm no Brigade requirement | Premises or Contacts (122) |

Should a Fire Authority response be required to fire alarm signals this must be specified on the monitoring application form.

Fire Authority responses may be subject to individual Fire Authority filtering policies as per the Chief Fire Officers Authority (CFOA) CFOA Code Practice. A list of the fire authorities that use filtering is available from our ARC administration department.

It may be necessary to contact the premises prior to contact with the Fire Authority. If you have dispensation for the ARC not to call the premises, we will normally need a copy of the letter of authority from the Fire Brigade for the ARC to remove this facility.

Some Fire Authorities require Unique Reference Numbers (URN's) for the ARC to be able to dispatch calls to them.

Some Fire Authorities adopting the CFOA call challenge procedures may refuse to attend a Fire Alarm unless the customer/premises confirms they have a fire & furthermore these Brigades do not accept a 'no reply' as a confirmed situation.

In cases where open and close is monitored via the security system, we will normally not call the premises in response to a fire alarm when they are known to be closed.

If our response to fire alarm signals requires changing, we would normally expect to receive this instruction in writing.

### 5.7 Personal Attack/Hold-up Alarm Conditions

| Type of Alarm | Action taken by our ARC |
|---|---|
| Personal Attack Alarm | Police (200) |

It is our ARC policy that all PA's/Hold Up Alarm conditions are police-able immediately (no filter) with a valid police URN on level one police response. Normal Police rules apply see section 5.3.

#### 5.7.1 Confirmed hold-up alarms

BS 8243 sets out the requirements for confirmation of hold-up alarms where this is required under NPCC or Police Scotland policies. NPCC Policy states,

> *"3.4.4* For restoration of HUAs which have lost response, confirmation is mandatory.
>
> Note: telephone call-back as a single method of confirmation will not be accepted for reinstatement for systems installed in commercial premises".

Thereby Hold-up Alarm Systems (HAS) will be required to incorporate alarm confirmation technology to gain reinstatement of Police response should the PA URN become withdrawn.

#### 5.7.2 Types of confirmation

BS8243 clause 4.2.2 states:

> *"HAS's should incorporate one or a combination of the following alarm confirmation technologies:*
>
> *1 audio confirmation*
> *2 visual confirmation*
> *3 sequential confirmation*
> *4 telephone confirmation (call back)*
>
> *An explanation of the selected combinations should be provided to the user/client.*
>
> *The installer should obtain written confirmation of the client/user's acceptance of the chosen option, and detail how the confirmation works.*
>
> *NOTE: Confirmation of a HUA is not mandatory unless restoration of police response is required following false activations (see NPCC and ACPOS/PS security systems policies)".*

#### 1) Audio Confirmation

It must be clearly stated on the monitoring application form that audio confirmation is required of Hold-up Alarms and the type of confirmation used. We only accept audio systems with ring back, such as AV60.

Before commissioning the system please ensure the ARC is in receipt of a completed application form and the form states the type of audio verification system used and the telephone number which is to be used to dial up the system for alarm verification purposes.

| Default MasterMind Event Code Reference | ARC Alarm Response |
|---|---|
| 200AUD Personal Attack (Audio) | 1. Premises (via audio) and Police or Contacts<br>*(If no sound is heard or unable to connect to the audio system, pass to Contacts/Keyholders as an unconfirmed alarm. If sound is heard, pass to the police as a confirmed hold-up alarm)*<br>and/or<br>2. Police or Contacts |

### 2) Visual Confirmation

Where visual confirmation is required of Hold-up Alarms for systems designed to comply with BS5979 and BS8243 rather than BS8418, our specialist Remote Video Response Centre (SMC Vision) within the group should be contacted for further information, telephone: 0844 879 1007.
A typical response to a video confirmed hold-up alarms system is stated below.

| Default MasterMind Event Code Reference | ARC Alarm Response |
|---|---|
| 200VID Personal Attack (Video) | 1. Premises (via video) and Police or Contacts<br>*(If nothing seen or unable to connect to the video system, pass to Contacts/Keyholders as an unconfirmed alarm. If activity is seen, pass to the police as a confirmed hold-up alarm)*<br>and/or<br>2. Police or Contacts |

### 3) Sequential & Telephone Confirmation

For hold-up alarm conditions to be considered sequentially confirmed BS8243, clause 5.2.2 states:

> *"a) the HAS should be configured so that at least two separate alarm conditions are reported within the confirmation time; and*
>
> *b) signals emanating from HDs (hold-up devices) should be from either;*
>
> *1) two or more HDs separately identifiable at the CIE; or*
>
> *2) a multi action HD.*
>
> *The hold-up confirmation time should be not less than 8 hours and not more than 20 hours".*

It must be stated on the monitoring application form that sequential confirmation is required of Hold-up Alarms and the transmission protocol used. Before commissioning the system, please ensure the ARC is in receipt of a completed application form and the form states the type of sequential verification used and the alarm response required, i.e.

| Type | Unconfirmed HA | Confirmed HA |
|---|---|---|
| PA Second Zone Reporting | Unconfirmed HA<br>usually channel 2 | Confirmed HA<br>usually channel 7 |
| SIA Format | PA or HA Unconfirmed HA | HV Confirmed HA[1] |
| Ademco E Code | E120 Unconfirmed HA | E129 Confirmed HA[2] |

### 5.7.3 Default ARC Response

| 1. Hold-up alarm without alarm confirmation | | |
|---|---|---|
| **Alarm Event** | **Default MasterMind Event Code Reference** | **ARC Default Alarm Response** |
| Unconfirmed Hold-up (without telephone call back) on channel 2 or Ademco E code 'E120' or SIA 'PA' or 'HA' | 200<br>(Personal Attack) | Police Only |

[1] Mnemonics specified within Appendix A.7.3 of BS8243: 2021
[2] Mnemonics specified within Appendix A.7.3 of BS8243: 2021

| 2. Hold-up alarm with sequential alarm confirmation | | |
|---|---|---|
| **Alarm Event** | **Default MasterMind Event Code Reference** | **ARC Default Alarm Response** |
| Unconfirmed Hold-up on channel 2 or Ademco E code 'E120' or SIA 'PA' or 'HA' | 210BS (Personal Attack) *(where required for reinstatement of Police URN)* | Contacts only |
| Upgraded to Confirmed Hold-up through receipt of a confirmed alarm on channel 7 or Ademco E code 'E129' or SIA 'HV' | 200SCO *(Sequentially Confirmed Personal Attack Alarm)* | Police only *(as a confirmed personal attack alarm)* |

| 3. Hold-up alarm with sequential alarm confirmation and telephone call back* | | |
|---|---|---|
| **Alarm Event** | **Default MasterMind Event Code Reference** | **ARC Default Alarm Response** |
| Unconfirmed Hold-up (with telephone call back) on channel 2 or Ademco E code 'E120' or SIA 'PA' or 'HA' | 223BS (Personal Attack) | 1. Call Premises *(If no answer, pass to Contacts/ Keyholders. If answered and confirmed false alarm but unable to verify via password, pass to Contacts/Keyholders. If stated genuine pass to the police as a confirmed hold-up alarm)* and/or *2.* Police or Contacts |
| Upgraded to Confirmed Hold-up through receipt of a confirmed alarm on channel 7 or Ademco E code 'E129' or SIA 'HV' | 200SCO *(Sequentially Confirmed Personal Attack Alarm)* | Police only *(as a confirmed personal attack alarm)* |

***Note: In accordance with the NPCC policy, with effect from 1.4.2018 telephone call back as a single method of confirmation will not be acceptable for reinstatement for systems installed in commercial premises.**

The hold-up confirmation time configured by the alarm system control and indicating equipment (CIE) at the protected premises must not be less than 8 hours and not more than 20 hours. If at the expiry of the confirmation time HDs remain in an alarm condition and are inhibited[3] a signal should be sent from the CIE to the ARC.

Notes: 1. To function correctly and to minimise the likelihood of false alarms occurring a signal must be sent to monitoring centre when channels are restored to their quiescent state.
2. For systems sending SIA Protocol: If receipt of the 'HA' mnemonic should be interpreted as 'Duress' and passed to the Police, you must advise us of this on application otherwise it will be interpreted as an unconfirmed hold-up alarm.

| Zone Omit Signals | Zone Omit Signal | Default Alarm Response |
|---|---|---|
| Fast Format | Usually channel 6 | 610Z0 Contacts only |
| SIA Format | PB or HB | |
| Ademco E Code | E925 | |

To distinguish between a confirmed intruder alarm and a confirmed hold-up alarm for systems signalling both events via the same alarm channel, i.e. usually channel 7 for 'fast format', an extra event is attached to the system called 'CONFPA', this recognises, through interrogation of the previous alarm events, when the alarm should be processed as a confirmed hold-up event rather than a confirmed intruder event.

A failsafe default event code of '200SCO', as previously defined, is embedded within the monitoring centre alarm signal processing software should a confirmed alarm signal follow an unconfirmed hold-up alarm and the 'CONFPA' event has not been specified.

[3] Reference BS8243: 2021 Appendix A.7.2

### 5.7.4 Alarm Combinations

Alarm Systems signalling limited information content, e.g. fast format, the upgrade to a confirmed alarm will be made on the following basis.

| First Signal | Subsequent Signal (usually channel 7) | Alarm Designation |
|---|---|---|
| HU Alarm | Confirmed Alarm | Confirmed Hold-up Alarm |
| Intruder Alarm | Confirmed Alarm | Confirmed Intruder Alarm |
| Tamper Alarm | Confirmed Alarm | Confirmed Intruder Alarm |
| Hold-Up Alarm & an Intruder Alarm in either order | Confirmed Alarm | Confirmed Hold-up Alarm |
| Hold-up Alarm & a Tamper Alarm in either order | Confirmed Alarm | Confirmed Hold-up Alarm |
| Hold-up Alarm & a Transmission Fault in either order | Confirmed Alarm | Confirmed Hold-up Alarm |
| Intruder Alarm & a Tamper Alarm in either order | Confirmed Alarm | Confirmed Intruder Alarm |

Note: Dual path signalling is optional under BS8243, clause 4.3.

For the purpose of confirmation of hold-up alarms in conjunction with transmission faults, the internal confirmation time of the monitoring platform has been set to 20 hours.

### 5.7.5 System Designation

As of 1st July 2022, new systems that specify confirmation of hold-up alarms will attract an alarm response to the requirements of BS8243: 2021 and PD6662: 2017 unless we are instructed otherwise.

If confirmation of hold-up alarms is not specified, our default response plan, event code 200, will be applied and unconfirmed hold-up alarms will be passed to the police.

It is important to ensure that we are informed of new systems that should receive an alarm response to an earlier standard than BS8243: 2021 and PD6662: 2017 and of existing systems that are upgraded to current standards and should have their response plan changed.

### 5.8 Intruder Alarms

| Type of Alarm | Action taken by the ARC |
|---|---|
| Unconfirmed Intruder Alarm | Premises & Contacts (Contacts) - (1322OC) |
| Confirmed Intruder Alarm when closed within re-arm period or audio or visual verification | Police and Contacts (1380) (as confirmed) |
| Confirmed Intruder Alarm when open | Premises or Contacts (1380) |
| Unconfirmed Intruder alarm followed by an Open or Abort signal | No action taken (1322OC) |
| Sequentially Confirmed Intruder Alarm received within the filter period of the initial Unconfirmed Intruder alarm followed by an Open or Abort signal | No action taken (1380) |

All police calling systems must have a unique reference number (URN) for the ARC to be able to dispatch to them and be on level one police response.

All new intruder alarm systems installed within an NPCC or Police Scotland Authority Area that require a police response and systems that have had police response withdrawn but now require police response reinstating must incorporate confirmation technology.

All intruder alarm signals received from sequential confirmed intruder alarm systems within premises residing in NPCC or Police Scotland Authority Areas are held for 120 seconds in order that they may be aborted or confirmed by a second detector.

### 5.8.1 Southern Ireland Only

All intruder alarm signals received from sequential confirmed intruder alarm systems within the Garda Siochana Police Authority Areas are held for 60 seconds in order that they may be aborted or confirmed by a second detector.

The Company may enter into an agreement with the end user to modify alarm responses to the first alarm signal:

i.e. take no action on the first signal.

The Company should ensure the End-User has a copy of the ARC Filtering Policy and has entered into an agreement to accept the stated response. It is anticipated that the relevant filtering policy may be extracted from this manual by the Company for their tailored use. The amended response must be conveyed to the ARC on our standard connection form.

## 5.9 Types of Confirmed Intruder Alarm

### 5.9.1 Sequentially Confirmed Alarms

Sequential alarms are perhaps one of the simplest confirmation technologies. The ARC just needs to know that two independent detectors or two detectors of different technologies have activated within the protected premises.

Signals are held for an intentional delay of 120 seconds for premises residing within NPCC or Police Scotland Authority Area's in order that they may be aborted or confirmed by a second detector.

Should a confirmed intruder alarm signal be received within the alarm filter period of the initial alarm, on expiry of the initial filter time the alarm is presented to an operator for action as a confirmed alarm.

Should the End User send a mis-operation signal or a signal to indicate the system is unset prior to any action by the ARC the alarm will normally be automatically aborted.

It is important that alarm systems incorporating sequential confirmation are set to re-arm within a time window (30 - 60 minutes) following initial activation to prevent the transmission of a confirmed alarm signal and to prevent the ARC from carrying out the incorrect action on any subsequent activation. Should the zone that generated the initial unconfirmed alarm be isolated on re-arm then a signal should be sent to the ARC to indicate a zone has been omitted. This will then be reported as stated in section 5.25.

### 5.9.2 Southern Ireland Only

Signals are held for a minimum of 60 seconds for premises residing within the Garda Siochana Police Authority Area's in order that they may be aborted or confirmed by a second detector.

### 5.9.3 Type of Sequentially Confirmed Alarm

| Type | Unconfirmed Signal | Confirmed Signal |
|---|---|---|
| Second Zone Reporting | Unconfirmed Intruder usually channel 3 | Confirmed Intruder usually channel 7 |
| SIA Format | BA Unconfirmed Intruder | BV Confirmed Intruder |
| Ademco E Code | E130 Unconfirmed Intruder | E139 Confirmed Intruder |

A confirmed signal must be delivered by the appropriate mnemonic code within the protocol used, the ARC will not accept ‘any’ second event as a confirmed alarm condition and for second zone reporting the channels for the unconfirmed and confirmed intruder signal must be pre-designated on application to the ARC.

### 5.9.4 Open & Close signals with Point ID and SIA

It is strongly recommended that open/close signals are enabled to the ARC when using Point ID and SIA. In the event the Company wishes to disable open/close thorough checks must be made by the Company to ensure all associated signals are also disabled when commissioning the site.

For example the “OR” command in SIA (Open after an alarm) may change the status of the system to Open and therefore make the system non-policeable.

If you wish to send additional signals such as the “OR” command as an abort without sending open/close you must instruct the ARC to create an additional zone per event specifically for this purpose.

Example

OR = Abort =1399

If “OR” command is programmed correctly and it is received within 120 seconds following an intruder alarm, the alarm may be aborted correctly without changing the status of the alarm system at the ARC.

It is the Company’s responsibility to ensure that every element of the connection is tested with the ARC and the response required is confirmed.

It is imperative when changing control panel suppliers that a full test is carried out with the ARC to ensure the connectivity and response required is correct.

The ARC cannot accept any responsibility for Point ID and SIA systems where the open/close signals are disabled and associated zones are left enabled with no additional zones being created.

### 5.9.5 Audibly Confirmed Alarms

Audio confirmation requires the ARC to listen to audio data from the protected premises following the receipt of unconfirmed intruder alarm signals. We only accept audio systems with ring back, such as the AV60.

Before attending site please ensure that ARC is in receipt of a completed TouchForm and the form states the type of audio verification system used and the telephone number which is to be used to dial up the system for alarm verification purposes.

The ARC should be contacted prior to the system being connected to place the system in-service and on-test.

Testing of all microphones should be carried out in local mode by the engineer on site in accordance with the manufacturers’ recommendations.

When you are satisfied with the audio coverage, the ARC should be contacted to carry out a test dial into the site to ensure the system is working correctly and sounds can be heard.

For compliance with pre BS8243:2021, audio systems must incorporate technology capable of detecting and signalling to the ARC a sequential confirmation alarm should two detectors activate that meet the sequential confirmed requirements of this code of practice. BS8243:2021 clause 4.2 states:

*“Alarm signals can be confirmed in a number of ways but, typically, they fall into two categories:*

*a) confirmed by the CIE, e.g., by processing sequential alarms; or*
*b) confirmed by an ARC or ARC operator, e.g., by listening, talking and/or viewing.*

*Where confirmation is determined by an operator, there might be an element of subjectivity surrounding what is heard or seen. In these circumstances, the operator is advised not to call the emergency services unless there is positive evidence of crime in progress.”*

Should a sound be heard then we will treat as a confirmed alarm. The ARC will not use discretion. Under normal circumstances, our ARC undertakes the following time guidelines:

| Service | Setting |
|---|---|
| Pre Alarm | 10 seconds |
| Post Alarm | 20 seconds |
| Real Time | 30 seconds |

The maximum time our ARC agent should listen is one minute. The Company must ensure audio systems are configured to provide this response to ensure the alarm receives the correct action by the ARC. All audio systems must send open/close signals to the ARC.

### 5.9.6 Visually Confirmed Systems (SMC Vision)

We provide CCTV monitoring through one specialist Remote Video Response Centre (SMC Vision) within the group. For further information, please contact 0844 879 1007.

For systems designed to comply with BS5979 and pre BS8243:2021 rather than BS8418, Video systems must incorporate technology capable of detecting and signalling to the ARC a sequential confirmation alarm should two detectors activate that meet the sequential confirmed requirements. Such systems installed in compliance with BS8243:2021 must be configured as specified within 5.9.2 above.

### 5.10 Path Failure Alarm Conditions

EN50131 and EN50136 calls for signalling suppliers to report line failures to the ARC in the following timings.

| EN50136-1:2018/PD6669:2017* | | | Equivalent Legacy Grade | |
|---|---|---|---|---|
| **Single Path** | **Dual Path** | **Failure Reporting Within** | **Grade** | **Failure Reporting Within** |
| SP2 | DP1 | 25 Hours | 2 | 25 Hours |
| SP3 | DP2 | 31 Minutes | 3 | 60 Minutes |
| *SP3+ | *DP2+ | 11 Minutes | 3 | 60 Minutes |
| N/A | DP3 | 4 Minutes | 4 | 6 Minutes |
| SP4 | DP4 | 3 Minutes | 4 | 6 Minutes |
| SP5 | N/A | 90 Seconds | N/A | N/A |
| SP6 | N/A | 20 Seconds | N/A | N/A |

Signalling supplier's interpretation of this standard may be different depending on grade and supplier. Please check with your nominated supplier for the reporting times by grade.

The ARC will only respond to path failures received by the monitoring software (MAS) as documented below unless otherwise instructed by the company or end-user or the site has become troublesome as detailed in section 5.15. Changes to response must be documented in writing.

| Type of Alarm | Status | Standard Response |
|---|---|---|
| Single Path Failure (1 Unconfirmed) | Open | Report notification via email/text* (alarm company or customer) (xxLOG) |
| Single Path failure with a single intruder or vice versa or dual path failure (2 unconfirmed) – see note 1 | Open | Premises or Contacts (390) |
| Dual Path Failures (2 Unconfirmed) | Open | Premises or Contacts (522xx) |
| Single Path Failures (1 Unconfirmed) | Closed | Report notification via email/text* (alarm company or customer) (xxLOG) |
| Single Path failure with a single intruder or vice versa or dual path failure (2 unconfirmed) – see note 1 | Closed | Police and Contacts (390) (as confirmed) |
| Examples of xxLOG given in the below tables, namely PALOG, FALOG, INTLOG etc. | | |

***Text messages are dispatched upon signal receipt at the ARC, prompt receipt of these messages are dependent on the signal availability to your device.***

1. To enable police attendance both unconfirmed events must occur in a single set period not exceeding 96 hours.
2. For the upgrade path to work an extra zone requires creating at the ARC called CONF (390). This zone is not transmitted from site. It is an internal zone which drives the upgrade path for alarms/failures that would normally only be classed as unconfirmed. Removal of this zone would remove the upgrade service to the alarm system.
3. Systems that monitor path failures must also transmit open/close signals and restores without exception to the ARC. This is to ensure the correct response to path failures is carried out in accordance with clause 6.4.2 of BS5979. Care should be taken to ensure the open/close signals are working the correct way round.

Our ARC will accept no liability for incorrect actions where the open/close signals are working back to front.

4. The ARC may abort a response if the line failure restores in a reasonable time frame.
5. On receipt of restore signals the status of the corresponding path failure condition will be returned to its dormant state, the ARC will log this event but will not normally inform the End User of the status change and it is the responsibility of the End User to monitor reinstatement at the protected premises.
6. STU's that have temporarily lost power due to power supply problems may go into 'no-response'. Statistics from BT Redcare indicate that in only 2% of cases the use of the "UP STU" command results in the unit returning to normal. The use of the "UP STU" command also allows for the possibility of STU substitution in an attempt to compromise the system. Our ARC recommends that the "UP STU" command is only used on instruction from an alarm engineer who has previously placed the systems "on test" from the customer's premises. Our ARC will only "UP" a STU in response to an alarm event with a valid password or with prior written authorisation from the Company and we do not accept liability for any loss or error that may occur as a result of this action.
7. Single path failure conditions of EN50131 Grade 2 & 3 systems are normally filtered for 60 minutes and Grade 4 systems for 10 minutes in order that the alarm may be aborted through receipt of a restore signal to avoid unnecessary call to Keyholders.

All intruder alarm signals received from sequential confirmed intruder alarm systems within premises residing in NPCC or Police Scotland Authority Areas are held for 120 seconds in order that they may be aborted or confirmed by a second detector.

### 5.10.1 Southern Ireland Only

Where the alarm signalling and monitoring arrangements are such that a communication or transmission fault might possibly give rise to Garda Siochana call-out, the Company should advise the subscriber in writing at the time the alarm-monitoring agreement is being set up that communication or transmission faults that result in Garda Siochana call-out can adversely affect future Garda Siochana response to the alarm system.

### 5.10.2 Path Failure Reporting

Our ARC will normally advise the Company the next working day by report should a Path Failure remain in 'Fault' for greater than 24 hours. Systems set to 'log only' may not report. Our ARC considers that any 'duty of care' responsibilities to the Company in respect to systems exhibiting signal failure will have been fulfilled following the above actions. Reports can be run via SmartPAC to list all sites that are in path failure, (Reports/ Management/Unrestored Alarms/NRs/LFs).

### 5.11 Fault and Other Advisory Alarm Conditions

Following the increased signalling requirements of EN50131 the number of signals to be sent to the ARC have noticeably increased, especially those categorised as low priority or advisory.

Customers should recognise these low level alarms as 'advisory events' and in many cases, dependent upon their circumstances, either an immediate automated notification method will be adopted, i.e. by text*, email, telephone, or these events are recorded in a report log for subsequent review by the alarm maintainer.

The default response to a range of fault and advisory events is stated in the following tables.

These signals are treated as low priority and may attract an extended filter period; if the signal restores in the delay period this may abort the alarm condition and no action will be taken.
Note: Some panel manufacturers may delay the transmission of AC mains fail & low battery to the ARC.

| Type of Alarm | Action taken by our ARC | | Filter period |
|---|---|---|---|
| | Premises Open | Premises Closed (or unknown) | EN50131 Grades 2,3 & 4 |
| AC Mains Fail | Premises or Contacts | Premises or Contacts (622MF) | 60 minutes |
| Low Battery Grade 4 | Premises or Contacts | Premises or Contacts (622LB) | 60 minutes |

| Type of Alarm | Action taken by our ARC | | Filter period |
|---|---|---|---|
| | Premises Open | Premises Closed (or unknown) | EN50131 Grades 2,3 & 4 |
| Low Battery Grade 2 & 3 & Non Graded | By Report Only | By Report Only (LBLOG) | N/A |
| Tamper | Premises or Contacts | Contacts (622TA) | 60 minutes |
| System Fault | Premises or Contacts | Contacts (622SF) | 60 minutes |
| General Undefined Trouble Signals | Premises or Contacts | Contacts (622) | 60 minutes |

In line with customer feedback we have made provision for almost any alarm to attract a 'by report only' response and unless otherwise specified the following events will be set to "log only – by report" and will not normally receive the attention of an ARC operator.

| Type | Description | Log ONLY event |
|---|---|---|
| Communications Path | GSM Radio Fail (Zn 8) | GFLOG |
| Open/Close | Open/Close | 34 Open/35 Close Reportable on request |
| Polling | Poll Failure | 540DPF/522DP |
| TEST option | GSM Path TEST | ATSG |
| TEST option | Land Line Path TEST | ATSL |
| Trouble | Low Battery | AHS002/LBLOG |
| Unexpected event | Unknown | UNKLOG |

All these events are available by report for the Company to view the next working day as necessary. It is the Company's responsibility to action these events to the end-user where applicable and to ensure corrective actions are carried out as required where required.

Where the event is a trouble, polling, communications path or other unexpected event, it is recommended that a full test of the alarm system including every zone and all signalling paths is carried out to the ARC for each alarm and restore channel.

The following events are available as 'LOG only – By report' where requested:

| Type | Normal Event | Description | Log ONLY event | Restore |
|---|---|---|---|---|
| 0 UNKNOWN | 1000 | NOT USED OR SETUP | UNKLOG | |
| 1 FIRE | 101 | FIRE ALARM | FALOG | |
| 2 PA | 200 | PERSONAL ATTACK | PALOG | |
| 3 INT | 1322 | INTRUDER | INTLOG | |
| 3 INT | 1380 | INTRUDER CONFIRMED | CONLOG | |
| 4 COMMS | 522DGF | GPRS FAIL | GPRLOG | 2000DG |
| 4 COMMS | 522GN | GSM FAIL | GNLOG | |
| 4 COMMS | GFLOG | GSM RADIO FAIL | Log as Standard | 520GR |
| 4 COMMS | 522IP | IP FAIL | IPLOG | 2000IP |
| 4 COMMS | 522PK | PAKNET PATH FAIL | PKLOG | 520PR |
| 5 NO RESPONSE | 522BT | BT PATH FAIL | BTLOG | |
| 5 NO RESPONSE | 522NR | NO REPONSE | NRLOG | |
| 6 TROUBLE | 622MF | AC MAINS FAILURE | MFLOG | 699MFR |
| 6 TROUBLE | 622AM | ANTI MASK | AMLOG | |
| 6 TROUBLE | 622LB | LOW BATTERY | LBLOG | 699LBR |
| 6 TROUBLE | 622SF | SYSTEM FAULT | SFLOG | 699SFR |
| 6 TROUBLE | 622TA | TAMPER | TALOG | 699TAR |
| 6 TROUBLE | 610ZO | ZONE OMIT | ZOLOG | |
| 7 LINK DWN | 522GL | GSM LINK DOWN | GLLOG | |
| 7 LINK DWN | 522GL | LINK DOWN | LDLOG | |
| 8 POLLING | 522LP | DUALCOM POLL FAIL | Log as Standard | |

| Type | Normal Event | Description | Log ONLY event | Restore |
|---|---|---|---|---|
| 8 POLLING | 540DPF | GPRS POLL FAIL | GPPRPT | 2000DP |
| 9 TEST | ATSG | GSM PATH TEST | Log as Standard | |
| 9 TEST | ATSL | LANDLINE TEST | Log as Standard | |
| 9 TEST | TTFLOG | TIMER TEST | Log as Standard | |

The Following Events are LOG only when Open: CO – Contacts only when closed

| Type | Normal Event | Description | Log when OPEN | Restore |
|---|---|---|---|---|
| 1 FIRE | 101 | FIRE ALARM | 110CL | |
| 3 INT | 1322OC | INTRUDER | 1310CL | |
| 4 COMMS | 522GN | GSM FAIL | 510GNC | |
| 4 COMMS | GFLOG | GSM RADIO FAIL | 510GFC | 520GR |
| 5 NO RESPONSE | 522NR | NO REPONSE | 510NRC | |
| 6 TROUBLE | 622MF | AC MAINS FAILURE | 610MFC | 699MFR |
| 7 LINK DWN | 522LD | LINK DOWN | 510LDC | |

The Following Events are LOG only when Open: Actions as stated when closed

| Type | Normal Event | Description | Log when OPEN | Closed Act. |
|---|---|---|---|---|
| 1 FIRE | 101 | FIRE ALARM | 101CL | FB,CO |
| 2 PA | 200 | PERSONAL ATTACK | 200CL | PF |
| 3 INT | 1304 | INTRUDER | 1304CL | PF,CO |
| 3 INT | 1380 | INTRUDER CONFIRMED | 1380CL | PF,CO |
| 4 COMMS | 390 | CONF (NR + INT) | 390CL | PF,CO |

Events should not be changed to LOG ONLY without being reportable.

As part of SMC Custodian's continuous improvement program, all faults & advisory signals may be notified utilising an intelligent automated process, e.g. by telephone, email or text* services.

### 5.12 Linkdown Message

"Linkdown" is a message sent to the ARC if the BT Scanner in the exchange has lost connectivity with the subscriber transmission device (STU) normally through planned outages on the BT Redcare network. Our operational teams suspend these "Link Down" messages normally from 60 to 120 minutes depending on the severity of the volume of alarms as the majority do restore (Link OK) in this time. This could in some circumstances effect the transmission of the GSM also.
As a duty of care if we do not see the "Link OK" in a reasonable time frame we will notify the customer of the situation.

### 5.13 Late Restoral Alarm Conditions (LRAC)

BS8243 requires all intruder & Hold-up signalling systems to send restores without exception. All connections should be commissioned with the zones working the correct way round. It is bad practice to ask the ARC to invert the response and act on restores.

The majority of intruder and path failure conditions that have failed to restore in approximately 90 minutes from full clearing the alarm condition may be reported by the LRAC processing. The LRAC processing is a reportable service and is accessible for review via SmartPAC Reports.

When the Company identifies an LRAC, they should proceed to restore the alarm condition as soon as possible.

Where the LRAC is a path failure this may take longer to rectify by the path supplier but still needs the company's attention. Until the alarm zone is restored, the ARC may not be in a position to action any further alarm conditions from that zone or zones, this includes path failure alarms.

### 5.14 Systems with Opening and Closing Time Schedules

Our ARC offers to monitor open and close against a time schedule normally at an additional cost.

LTC – Late to Close (Additional charges may apply)
ETO – Early to Open (Additional charges may apply)

### 5.14.1 Automated Late to Close (LTC) & Early to Open (ETO) Reminders

Response to LTC & ETO reminders would normally be from the automated service whereby the premises will receive either, an automated telephone call, text* or email.

| Type of Alarm | Action taken by our ARC |
|---|---|
| Early to Open – ETO<br>***or***<br>Late to Close - LTO<br>(more than 30 minutes before scheduled opening time) | Premises or Contacts |

Should the status change before the ARC has dispatched the reminder the incident will be treated as complete and no further action will take place.

If the ETO reminder is generated in response to a previous alarm condition notified to the Contact/Keyholder no challenge will be made by the ARC in response to the ETO. If the Contact/Keyholder is under duress they should use a PA or enter a duress code when entering the protected premises.

### 5.15 Digital Communicator – Timer Tests

Systems communicating via Digital Communicators that are required to signal to the ARC every 25 hours to meet the requirements of EN50131 should be configured to send daily timer test signals. The ARC monitoring system will normally log these signals and should a Digital Communicator fail to signal, the Company should run a report via SmartPAC to identify these systems.

Alternatively, the ARC can respond to missed 'Timer Test' signals and inform the Company in a similar way to any other transmission fault, but there may be an additional charge for this service.

### 5.16 Unknown Signals

If the ARC receives signals from a site/customer but the signal is unknown to the ARC we will normally notify the Company by CDO the next working day, create a zone for the unknown event and set the response to report only. From this point forward, every time this unknown alarm is received at the ARC the Company should be notified by normal reporting.

### 5.17 Excessive Signals

The ARC monitors excessive alarm signal traffic (except for those assigned as a 'log only' event). Should a particular site/system become 'troublesome', through the receipt at the ARC of unknown signals, unwanted signals or repetitive alarm incidents, we will normally inform the company of the site affected. Our ARC reserves the right to charge for excessive signal traffic & assign such signals as 'log only' events.

### 5.18 Calling Contacts/Keyholders

There should be a minimum of two Contacts/Keyholders available 24 hours a day for seven days per week with 1 contact being a mobile telephone number as a minimum requirement, in accordance with NPCC requirements. A 24-hour keyholding service can be utilised as one of the two required Contacts/Keyholders. To maintain operational efficiencies and to avoid extended delays in alarm response we recommend that there is a maximum of four Keyholders.

Each Contact/Keyholder should have transport available and reside within 20 minutes travelling distance of the protected premises. It is the Customer's/End User's/Company's responsibility to ensure the Contacts/Keyholders are maintained with the correct telephone numbers and sequence details on the ARC database.

1. We will ring for approximately 30 seconds before terminating the call during the day (0700 -1859 hours) and proceeding through the contact list
2. We will ring for approximately 60 seconds before terminating the call during the night (0000 -0659 and 1900 - 2359 hours) and proceeding through the contact list.
3. If Contacts/Keyholders are unavailable at the time of the incident we will suspend the incident for a minimum of 20 minutes and we may make further attempts to contact them up to but not exceeding one hour after the event, depending upon operational conditions at that time.
4. Answer phones are not normally considered an acceptable form of contact.

5. In the event that the ARC has been unable to speak to an authorised Contact/Keyholder, the ARC will normally send a text* message for the first Contact/Keyholder and notify the Company by report the next working day that all Contacts/Keyholders were unavailable.
6. When the ARC initiates the telephone call to the Contact/Keyholder we normally ask for the named contact but we don't require a password at this point.
7. Once a legitimate Contact/Keyholder has been contacted the incident will be closed. Should a Contact/Keyholder decline to attend the premises it will be their responsibility to contact another authorised Contact/Keyholder.
8. It is recommended that Contacts/Keyholders 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.
9. It is the Customer / End-user / Company's responsibility to ensure the attending Contacts/Keyholders are trained and are fully conversant with alarm terminology used by the ARC.
10. The ARC cannot advise on what actions the Contact/Keyholder should make. It is recommended if the ARC calls a Contact/Keyholder they attend the protected premises without exception.
11. Contacts/Keyholders should be advised that for disaster recovery purposes we use non-geographic numbers for passing alarm calls and our numbers must not be placed on restriction with their telephone service.

    ARC presentation numbers: 0844 879 1703, 0844 879 1719 & 0844 879 1720

The above requirements apply to all types of alarm signals that require site attendance. The response to an alarm event by the ARC may be made by an ARC agent telephoning the authorised Contact/Keyholder or form part of an automated process.

### 5.18.1 Automation of Incident Response

To improve efficiency and to provide a quicker response to alarm incidents we use an automated process for dialling Keyholders, this results in the ARC Agent only becoming involved once a successful call is made at the time the keyholder answers the telephone.

Please see Appendix B for details of the Operator Assist process.

### 5.19 Calling Premises

There are two premises' telephone number fields available on the monitoring database and only premises' telephone numbers should be contained in these fields. Under no circumstances should the premises number be inserted in the keyholder fields as this may cause confusion for the dispatch staff and may render the password not being requested which is a security risk.

If the premises number is requested to be contacted as part of the call plan the following rules apply:

1. Each number entered in the premises telephone number field will normally be rung for up to and not exceeding one minute.
2. If an answer phone is encountered, we will not leave a message. We continue with the call plan.
3. We will normally request a password to verify the identity of an authorised user for security related incidents, for non-security related incidents a password is not normally required.
4. It is the Customer/End-user/Company's' responsibility to ensure these numbers are kept up to date.
5. It is strongly recommended these numbers are not call forwarded to another destination as this may lead to the ARC not asking for a password at the correct point.

Note: Normally telephone numbers of the protected premises should be listed against the site details only and must not be duplicated as Keyholders.

### 5.20 Adverse Weather & Unforeseen Circumstances

### 5.20.1 Operations Team

Our ARC maintains operating levels to meet normal fluctuations of alarm signal traffic and have contingency plans in place should alarm signals reach unacceptable levels. In adverse and unforeseen circumstances, notably through severe weather conditions, extended power / network failures or National/Global Emergencies including epidemics or pandemics where signals received may exceed the number of operators available, the alarm queue will be managed;

- Our operators will prioritize the following high priority signals: Telecare, Fire Alarms, PA, Lone Worker and confirmed intruder where a valid URN is in place. All other signals will be automated which means that text* messages will be sent to keyholders informing them of any activations outside of the above priority signals.
- In the case of CCTV, subject to the volume of activations at any given time we will introduce a revised amount of allowable false alarms to a maximum of three in an hour (false and unwanted). Once the system has reached this limit it will be isolated and a fault report sent to the Company until the cause is resolved.

Important Actions to note:

1. Please ensure keyholders are made aware of those activations as detailed above which will be notified in text* format.

2. Please check all keyholder details to establish which do not have a mobile number and provide us with one for those that don't. Updates should be made via the TOUCH portal. If you use a keyholding company this may require you to agree with your keyholding company for them to provide a mobile phone number for this purpose.

### 5.20.2 Customer Support Team

In line with the contingency plans above, the Customer support team could be in a position whereby remote working capabilities are mobilised. This will enable the team to continue to access our systems for inputting changes, updates and ordering of signaling devices. Unfortunately, due to our customer support teams working remotely from home, waiting times on our phone lines could be longer than normal (including for data amendments), and we need your help to prioritize the most important calls and requests. Therefore, we would ask you to please use TOUCH to make simple changes and updates to your keyholder details. Please only contact us if you are unable to use TOUCH.

If you do not have TOUCH, please register at smc-touch.co.uk/registration

### 5.20.3 In the Event of Centre Closure

We will endeavor to activate the following support:

- Remote working for customer support team.
- Operations will only action the following critical signals: Telecare, Fire Alarms, PA, Lone Worker and confirmed intruder.
- In the case of CCTV, subject to the volume of activations at any given time we will introduce a revised amount of allowable false alarms to a maximum of three in an hour (false and unwanted). Once the system has reached this limit it will be isolated and a fault report sent to the Company until the cause is resolved.
- Non-essential services such as out-of-hours call handling may not be available.

### 5.21 Mezzanine Services – Smart Response

Mezzanine is the automation of operator incidents where the alarms are low priority or repetitive.

This service uses the following methods of communication to inform the customer of the alarm incident.

| Number | Type of Communication | Confirmation | Confirmation Method |
|---|---|---|---|
| 1 | Text* (there may be an additional charge) | No | N/A |
| 2 | E-mail | No | N/A |
| 3 | IVR (Interactive Voice Response) A | No | N/A |
| 3 | IVR (Interactive Voice Response) B | Yes | Accept key |
| 3 | IVR (Interactive Voice Response) C | Yes | Pin Number |

We monitor the transmission of these services but cannot guarantee the delivery or receipt unless a service with a level of confirmation is utilised. Therefore non-confirmed services should only be used for information only. Any security based applications should use service 3C. The ARC does not accept any liability for the incorrect application being selected.

### 5.22 Multiple Signalling Sites/Systems

It is strongly recommended that for every signalling system only one site is associated. Connecting multiple signalling sites/systems can be very complex in nature and should be discouraged.

For example, a digital communicator signalling with two intruder sites shop 1 and shop 2.

| Zone | Description/Area |
|---|---|
| 1 | Fire – Shop 1 |
| 2 | PA – Shop 1 |
| 3 | Intruder [Unconfirmed] – Shop 1 |
| 4 | Open/Close – Shop 1 |
| 5 | AC Mains Fail – Shop 1 |
| 6 | Bypass/Omit – Shop 1 |
| 7 | Intruder [Confirmed] – Shop 1 |
| 8 | System Fault – Shop 1 |
| 9 | Intruder [Unconfirmed] – Shop 2 |
| 10 | Fire – Shop 2 |
| 11 | PA – Shop 2 |
| 12 | Open/Close – Shop 2 |
| 13 | AC Mains Fail – Shop 2 |
| 14 | Bypass/Omit – Shop 2 |
| 15 | Intruder [Confirmed] – Shop 2 |
| 16 | System Fault – Shop 2 |
| PT | 24 Hour Timer test |

The commission process would need to ensure that both areas are fully tested.

We accept no liability if sites are not fully commissioned to the ARC.

### 5.23 Multiple Path Failures (Flood Conditions - WebWay)

All networks are susceptible to disruption and occasionally this may affect a large number of remote locations monitored by the ARC. The potential impact on the operation is serious as multiple communications failures are reported to our agents simultaneously.

Flood condition identifies a mass network outage and protects the ARC from a flood of communication failures being delivered to operators. The end-user should benefit from unnecessary disturbance due to planned/unplanned network maintenance that does not compromise the integrity of their remote IAHS systems (where dual path systems have been deployed).

Activation of Flood automatically delivers a high level alarm to ARC support. The status of the sites affected are then monitored, and once the network outage has cleared Flood Condition is released.

Flood does not block the delivery of alarm activations from the protected premises to the operator (e.g. Fire, Intruder, Open, Close, Confirmed Intruder, etc.).

### 5.24 Reasonable Alarm Monitoring and Associated Charges

Some companies have connected additional alarm/activity that is not associated with the monitoring service the site was quoted, ordered, and invoiced for or the site has repeated failures that are not being addressed.

Our ARC reserves the right to charge for additional alarm/activity where excessive traffic is not fair and reasonable and deemed to be over and above normal expected levels.

### 5.25 Omit/Re-arm

There is a requirement under BS 8243:2021 in Annex A, Section A.7.2 – Additional Signals or Messages which states:

*"The CIE should have the means to provide the following notification signals or messages, additional to those required by BS EN 50131-1:*

*a) mis-operation signal;*
*b) confirmed alarm;*
*c) reinstatement; and*
*d) reinstatement including detector or HD inhibited.*

*If the unconfirmed alarm is generated by a tamper condition, a tamper signal only should be notified."*

Most Control Panel Units (CPU's) can send a signal to indicate that a zone has been inhibited (By-Passed or Omitted) but unfortunately they cannot disseminate between this being carried out manually (by the alarm user when setting their alarm system) or automatically (by the alarm panel following an alarm activation).

To comply with the above condition our processes for Zone Omit are as follows:

On receipt of a Zone Omit event the process checks that an intruder alarm condition has occurred in the previous 60 minutes, the system is closed and the intruder alarm was received within the same set period:

Process True: – Action to Contacts/Keyholders

Process False: – Log Only

### 5.26 Pre ACPO Responses

The following is our ARC standard alarm response plan for systems issued with a URN prior to ACPO 2000 or ACPOS 2002 (as amended 1st April 2005), which have not had their police response withdrawn.

| Service | Alarm Response |
|---|---|
| PA | Police |
| Intruder (Premises Closed) | Police & Contacts (Unconfirmed) |
| Open & Close | Log Only |
| Confirmed Intruder (Premises Closed) | Police & Contacts (Confirmed) |
| Confirmed Intruder (Premises Open) | Premises or Contacts |
| Redcare No Response (Premises Closed) | Police & Contacts |
| Redcare No Response (Premises Open) | Premises & Contacts |

Deviation from standard ARC default response plans is not recommended and could lead to an unwanted response for which the ARC cannot accept liability.

Companies must write to the ARC stating they wish to adopt the Pre ACPO response or a personalised response.

### 5.27 Suppression of Sites Reporting Continuous Signals

Any site found by an Agent to be generating continuous signals will be escalated internally where SMC will review the history for the site and confirm that it is signalling continuously and identify the zone or zones affected. Any site signalling three alarms or more on the same zone in any four-hour period will fall into this category.

Attempts will be made to contact an authorised person, if an authorised person is contacted they will be informed of the situation and that the individual zone will be placed on test for a period of at least twenty four hours but not exceeding seventy two hours. Failure to contact an authorised person will result in the zone / zones being suppressed for the above mentioned time periods. (When Alarm Suppression is utilised on the database, all signals from the affected zone or zones will be logged in the history as normal but WILL NOT be presented to an Agent for action). Comment to this effect will be inserted in the site history detailing the actions taken. Custodian will notify the alarm company of such suppressions through the normal CDO process.

After the test period or period of Alarm Suppression expires, the zone or zones will automatically come back into service and any further signals will be presented to an Agent. If the problem regarding the continuous problematic signals is not resolved, then the process is repeated.

# 6. Placing a System On or Off Test

### 6.1 Testing Conditions

It is imperative if a system is being tested by a customer/engineer that it is placed 'on test' prior to testing. This will ensure that whilst testing, an alarm event is not passed to an ARC Agent for action and the creation of a call to the emergency services in error.

Non adherence to the testing processes below has a detrimental effect on response times for genuine events; the ARC is unable to differentiate between genuine and non-genuine signals received. Should incidents of this nature occur the ARC is under no obligation to investigate instances where testing protocols have not been followed.

To assist with this process there are four options available.

1. Engineer testing (Using TOUCH - mobile phone application for engineers)
2. Engineer testing (Manual using 0844 telephone service)
3. Customer testing (Manual using 0844 telephone service)
4. Via SmartPAC and TOUCH – online 24/7

All monitored alarm systems must have a unique identifier number known as the CS number and an authorised password. Pre-booking a test with the ARC for a time in the future could be a security risk and should also be discouraged. Should a system require to be placed on test for longer than 24 hours a request for suspension of service must be made in writing as described within section 3.12.

Where weekly Fire Test schedules exist on the account, please ensure that the schedule is reviewed at least annually and any amendments are notified to the ARC.

If multiple tests are carried out by engineers and customers, care must be taken to ensure the tester does not override the other party's tests.

### 6.2 TOUCH for Engineers

TOUCH is unique to SMC Custodian and offers your engineers the ability to place sites on and off test and obtain remote resets without the need to make a call. With the use of a smart phone, PDA or tablet device, engineers can view alarm history and test results in real-time, providing visual confirmation that signals sent have been received by SMC Custodian. Refer to section 10.2 for further details.

### 6.3 TOUCH for Customers

TOUCH is unique to SMC Custodian and offers your customers the ability to place sites on and off test and obtain these test results. With the use of a smart phone, laptop or tablet device, customers can view alarm history and test results in real-time, providing visual confirmation that signals sent have been received by SMC Custodian. Refer to section 10.2 for further details.

During a fire alarm test all fire alarm signals received will be logged into alarm history without any operator intervention and should a different type of alarm occur during the test period, such as a Panic Alarm, the ARC will respond as a genuine alarm.

NOTE: Our computer will automatically take the system off test after the allowed time.

### 6.4 On Test Expiry Conditions

All test periods expire automatically at the time set upon the commencement of a test period or earlier if the Engineer/Customer contacts the ARC to complete the test.

If the ARC monitors restore conditions and a test automatically expires, but the system has not been restored and remains in alarm, such conditions will normally be reported to the party responsible for initiating the test so they can be reviewed. These incidents should be treated as high priority and the offending engineer/end-user provided with further training. The ARC will not accept any liability for tests that expire with unrestored alarm conditions.

# 7. Remote Restore (Remote Reset)

If you subscribe to this service, we may be able to control the restoring of your end user's alarm. Most manufacturers restore procedures can be accommodated by our ARC.

It is the Company's responsibility to ensure that the end user is fully instructed in the procedure for carrying out a remote restore and the circumstances under which a remote restore can be given.

### 7.1 Remote Restore Procedures

Following receipt by the ARC of a signalled alarm condition, the system may be restored remotely by the ARC (acting in conjunction with the user of the alarm system in attendance at the protected premises) and authorised by the ARC in accordance with BS8473.

Restoring in accordance with above shall only be authorised by our ARC if the following conditions are satisfied:

#### 7.1.1 Remote Restore (Not Policed)

When end user agreement has been obtained and authorised by an agreed security discipline (by exchange of predetermined codes, words or numbers).

The cause of the signalled alarm condition has been clearly described by the end user to the duty operator at the ARC and the description given is consistent with the alarm condition having been caused by client error or it was a genuine alarm.

The description of the cause of the signalled alarm condition is consistent with there being no requirement for an engineer’s visit.

For systems incorporating confirmation technology, the client at the alarm control equipment may restore unconfirmed alarms conditions without any reference to the ARC; refer to clause 10.1 of BS8473.

#### 7.1.2 Remote Restore (Policed)

When end user agreement has been obtained and authorised by an agreed security discipline (by exchange of predetermined codes, words or numbers).

The cause of the signalled alarm condition has been clearly described by the end user to the duty operator at the ARC and the description given is consistent with the alarm condition having been caused by client error; or the cause is known not to be with the alarm system.

It is our ARC policy not to remotely restore a genuine alarm that has been extended to the police due to the possibility of the end user’s insurance cover being invalidated should it be subsequently found that the alarm system is not fully working.

The description of the cause of the signalled alarm condition is consistent with there being no requirement for an engineer’s visit.

The number of alarms policed has not exceeded two within the last 12 Months.

Where remote restore is denied, the Company's Service Technician should visit the protected premises for the purpose of corrective maintenance and/or educating the user as appropriate.

The ARC will normally inform the Company as soon as possible, usually the next working day, of all signalled alarm conditions and the time and date of each remote restore.

### 7.2 Registration

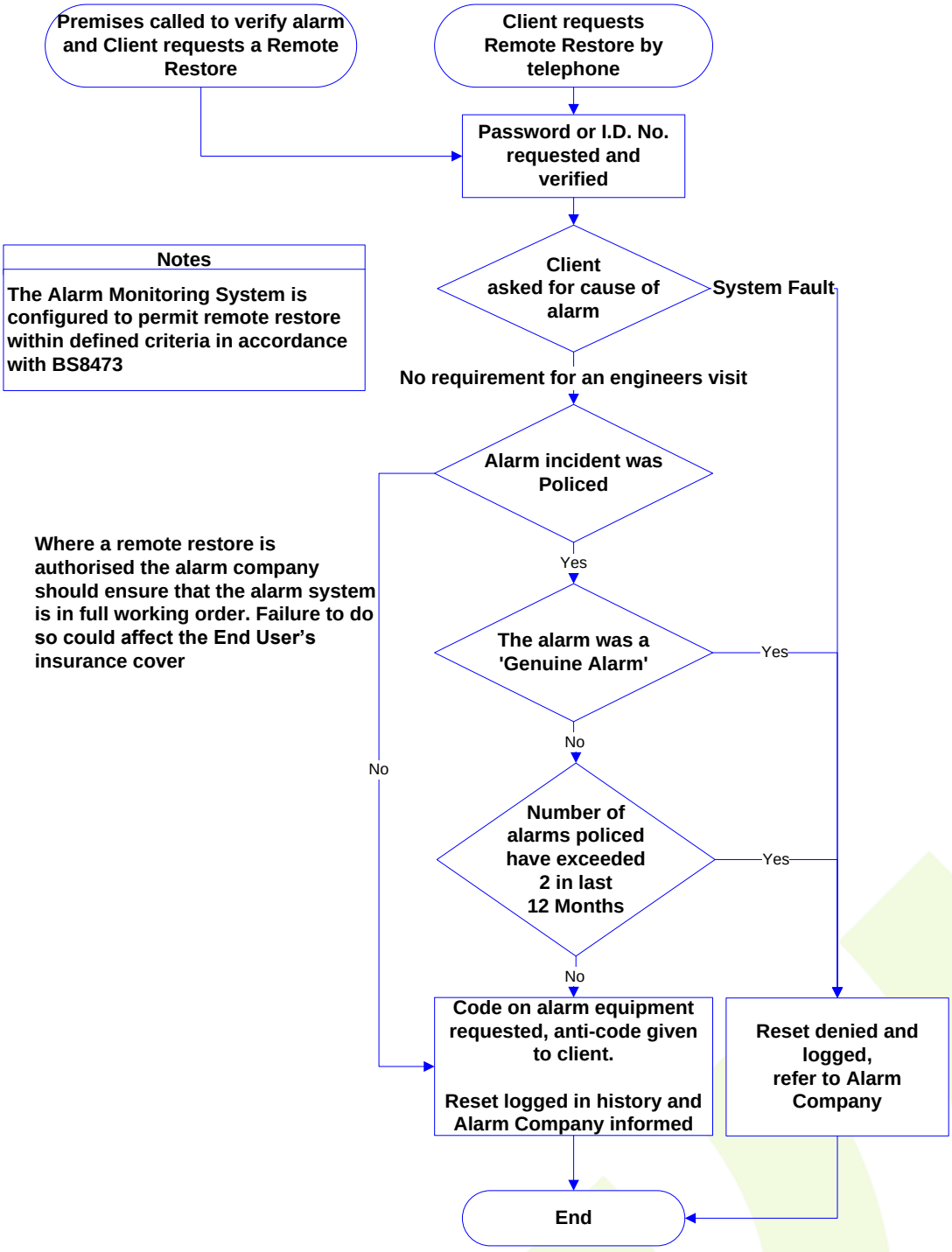
To register a system to allow Remote Restore to be carried out complete the relevant sections on the Monitoring Application Form, indicating which of the listed types of Remote Restore equipment has been installed and where appropriate, the SEED code number.

### 7.3 Remote Restore by Company

BS8473 permits the Company to designate its head office or branch offices as 'Restore Management Centres' and issue 'remote restores' to end users.

However, for the Company to carry out managed restores they must have access to the alarm history in order to determine if a managed restore is appropriate and must inform the ARC following the issue of any restore, the SmartPAC software suite available from our ARC may permit the Company to meet these requirements.

### 7.4 Remote Restore Flowchart



# 8. Company liability for accuracy of data held and system status at the ARC

### 8.1 Annual Audit

The correct management of the Company's data is critical and requires the highest level of management control by both the Company and the ARC. We strongly advise that at least once per year the Company carry out a critical data audit of the information held by the ARC for all its Monitored Systems, Company Engineers and Authorised Users, i.e. telephone numbers, URN's, Authorised Contacts & Keyholders, Passwords, etc. The ARC does 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 Company to the ARC
- Instructions that have been submitted on non-ARC recognised forms
- The receipt of ARC data change acknowledgements not being monitored by the Company
- Data changes submitted to the ARC not being checked for correctness by the Company
- Critical Data Omissions and other reports received not being addressed by the Company
- The ARC not being updated where and of the Company's details have changed
- Suspended alarm systems which have not been reinstated as a result of failure by the Company to notify the ARC

**The ARC will not be liable for any loss or error regarding the Company's data. It is the Company's responsibility to manage their data with the ARC.**

### 8.2 Company Maintenance & Corrective Actions Visits

These visits are an ideal time for the Company and the ARC to review and update end-user critical data such as:

1. Site data held by the ARC
2. Contact/Keyholder information
3. Status of response to the emergency services
4. Response to every zone
5. The zone configuration
6. System status (i.e. in-service or suspended)

The alarm signalling system to the ARC should be tested in full. Particular attention should be given to:

1. The open/close signals and whether they are working the correct way round
2. Whether the site is online and not suspended
3. Every zone which is being monitored
4. Path failure monitoring, where it is included, every communication path and dual monitoring failure should be tested. Most devices will normally have a single button that can be engaged to test all paths for maintenance purposes. Failure to test path failures and restores on maintenance visits may leave the signalling system in a failed mode rendering the systems on 'bells only'.
5. Contacts/Keyholders information and ensuring it is correct and will be called in the correct sequence.
6. The status of emergency service response is correct, i.e. Fire, PA & Intruder have the correct on/off response

The attending engineer should always check via TOUCH or with the ARC before leaving site to ensure all zones are clear (status clear) and the system is open / disarmed. Our ARC does not accept any liability for systems left on test status or un-restored when the engineer has left site.

### 8.3 Company review and action of ARC Reports

It is the Company's responsibility to ensure that reports detailed in sections 3.10 (Critical Data Omissions), 3.14 (Reports) & 5.11 (Fault & Other Advisory Alarm Conditions) - whether available via SmartPAC Reports or as received directly from the ARC - are reviewed to identify & amend any missing or incorrect data, should any incorrect data be found, the Company should notify the ARC immediately. Failure to do this could result in customers/end-users not receiving the correct alarm dispatch, information they have paid for or incurring additional cost. Our ARC will not accept any liability for failed alarm dispatch or telecommunications costs from a third party supplier or customers/end-users where reports have not been addressed with appropriate corrective actions.

# 9. Technical Information

### 9.1 Use of Alternative Call Providers

There have been some instances where delays have occurred in the transmission of alarm signals where alternative call providers, sometimes called Carrier Pre-Select, are utilised on lines servicing digital communicators.

Under normal circumstances, the digital communicator will initiate communication with the ARC receiver device with the sending of a “Hand Shake” tone, this must be acknowledged to the digital communicator within a set period of time, (which varies depending upon the digital communicator manufacturer).

The delay which can be introduced by the use of a Carrier Pre-Select vendor may cause the digital communicator not to receive the acknowledgement within the appropriate time. If this happens, the digital communicator will attempt to send another “Hand Shake”, at the same time as the acknowledgement is being returned. This results in both signals being unsuccessful.

It must therefore be ensured that communication devices are signalling correctly during commissioning and to identify existing sites that may be affected and investigate the occurrence of multiple entries in the ARC history by site for the same event. We have written a specific report on SmartPAC to identify such sites that may be affected, (Reports/History/Repeated Events in the last 24hrs).

If you identify a site that is affected there are three possible solutions as follows;

1. Prefix the dialled receiver number on the chip by 1280. This forces the call to be routed back to BT and therefore removes the delay.
2. Inform the customer to remove LCR (Least Cost Routing) from the affected line.
3. Provide an alternative line for the digital communicator to use.

Please note: this solution may not work for some suppliers.

### 9.2 Twenty First Century Network and NGN’s (Next Generation Networks)

Some communication companies have commenced the rollout of 21st Century Network (21CN) integrating various networks into one converged multi-service network. This could affect the communication path for some security transmission devices.

It is the Company’s responsibility to ensure that communication devices are compatible with the network.

### 9.3 Using Contact ID/SIA to Overcome 21CN and NGN’s Update

Traditional security signalling protocols like ‘Scancom Fast format’ and ‘Ademco Contact ID’ work on DTMF (dual tone multi frequency). This is where pairs of tones are sent down the line at a specific frequency and duration, the listening device (receiver) decodes these back to numbers.

A quote from the Ademco standard below shows that the tolerances are so tight (especially the kiss-off tone) that when a least cost or VoIP (Voice over IP) provider is introduced, there may be a slight delay with the signal being compressed, causing it to lose its timing/tone structure and fail to send:

*The handshake tone sequence shall consist of:*

- *A burst of 1400 Hz. ±3% tone with a duration of 100 msec. ±5%*
- *A pause of 100 msec. ±5%*
- *A burst of 2300 Hz. ±3% tone with a duration of 100 msec. ±5%*

*The Kiss-off tone from the receiver is used to tell the transmitter that the message has been received successfully. The frequency of the tone shall be 1400 Hz. ±3% and shall be sent by the receiver for a minimum of 750 msec. and a maximum period of 1 second. The transmitter must detect a minimum of 400 msec. of tone before considering the kiss-off to be valid.”*

In more modern signalling protocols like SIA, this has moved away from DTMF to FSK (Frequency Shift Key). This protocol is like a computer modem signalling with binary on and off. Because there are only 2 states to detect and not the 15 of DTMF, there a lot more chance of getting through.

Although SIA signalling can improve the 'hit rate' of a failing communicator, as they both use analogue sounds to transmit the signal, both are susceptible to timing and tone issue that come with some providers. It therefore cannot be considered a permanent fix and an alternative signalling system should be installed.

# 10. Product Support Software (Smart Suite)

The SmartPAC range of products has been developed for remote use by the Company to maintain control over their alarm systems and contribute to their business efficiency. SmartPAC permits the Company to manage and control data on-line, in real-time, accurately and confidently without the need for off-line verification within the requirements of BS5979 and BS8473.

### 10.1 SmartPAC

This facility provides real-time access to the Company's database. It enables amendments and additions to be made to Contact/Keyholder information, URN's / Status of URN's as well as making changes to a whole host of data including site details, etc. For further information email: custodian@smc-monitoring.com.

### 10.2 TOUCH (v1.0)

**Installers**: Allowing installers to remotely manage end user and engineer records, generate reports and place orders- live. Customize TOUCH, unique with your own branding and invite customers to use TOUCH and maintain their own records.

**Engineers:** Offers engineers the ability to place sites on and off test and obtain remote resets without the need to make a call. View alarm history and test results in real-time, proving visual confirmation that signals sent have been received by Custodian.

**End Users:** Allows end-users secure access to their account to make changes to keyholders, authorised users and passwords, view event history and generate key reports.

For further benefits and to register: smc-touch.co.uk/registration

### 10.3 TouchForms

This facility provides a suite of electronic forms which can be viewed and completed via a web browser and will send details directly to our ARC Administration.

### 10.4 Touch (v2.0)

Our commitment to innovation and developing market-leading technological solutions means we provide our customers with security monitoring services which improve performance and allow installers to deliver the best possible service. As a result, we have launched Touch v2.0, an upgraded and enhanced version of our original Touch Web portal. Installers can request registration as a Super User for Touch v2.0 at https://smc-touch.co.uk/registration. Requests should be submitted using an email address that includes the company domain wherever possible.

#### 10.4.1 Touch v2.0 Features

- Two factor authentication
- Speedy log-in with no need to use memorable information
- Self-managed password resets
- Health check dashboard with infographics & downloadable reports
- Ability to interrogate dashboard info in real time
- Ability to create, amend & remove users yourself
- Ability to select specific permissions & authority levels for other users (Superusers only)
- Easy drag & drop interface to add, remove & rearrange keyholders & authorised persons
- Site password & ALT ID changes
- Ability to suspend & unsuspend sites
- Keyholder creation & modification
- Keyholder schedules & suspend options
- Multiple site filtering options
- Option to place systems or site specific zones on test for non-engineers with no need for VRT calls

- Full site details including URN and brigade details in one place
- Detailed event history including timeline
- Show zone information, status & event actions
- View on test history
- Engineer system commissioning
- Orders & cancellations via TouchForms
- 90 days forced password change

### 10.5 Touch (v2.0) New User Authority Levels & Permissions

A key feature of Touch (v2.0) is to provide greater user control by giving the ability to create or disable new users, assign permission levels and reset passwords autonomously if registered as a Super User. Super Users can amend permissions in any arrangement that they chose.

Please note that Corporate, End Users and Users must be created by an Installers Super User, not SMC, to ensure data security, control of permissions and that access is only given to relevant sites.

Full details of how to create and disable Users can be found on the Touch Homepage once registered, along with other useful information and Frequently Asked Questions.

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

- Incorrect User creations, access or permissions
- Failure to disable user access when no longer required
- Data/instructions that have not been confirmed in writing by the Alarm Company
- Where instructions have been submitted on non-SMC recognised forms
- Where the Alarm Company has not monitored the receipt of SMC data change acknowledgements or has not audited received acknowledgements for correctness
- Where incorrect entries have been made on TOUCH
- Where systems have been incorrectly commissioned by the installer using Touch

For further details as to how we use personal information please go to:

GDPR (SMC : UK)

# 11. Additional Services

### 11.1 Out of Hours Emergency Demand Service Calls

Our ARC is able to offer under a separate contract an additional chargeable service to the Company for the handling of service requests from their clients outside of normal working hours. This service has the following benefits:

- **Facility** - Dedicated 0844 number answered by our professional Customer Service Agents, in the name of your company.
- **Procedure** – On receipt of a call from your customer, we will take their name, address, contact name and number plus particulars regarding the nature of their problem. These details will be entered onto our system, whereby a service job will then be raised. We shall contact the assigned engineer via our automated service dispatch. If we do not get confirmation from the engineer that they have received the call we will continue trying at 5 minute intervals for a period of 15 minutes. At this point we will revert to a backup engineer if one is in place with the same procedure. If after 30 minutes we have been unsuccessful contacting the duty engineer we may escalate to contacts that you specify.
- **Escalation Procedure** - An escalation procedure is required and be kept up-to-date should the ARC be unable to contact the duty engineer. If unsuccessful the outstanding call will be assigned to the company office and passed the next working day. If an escalation procedure is not present the outstanding call will be assigned to your office for the next working day.
- **Training** – Additional training on the use of TOUCH/SmartPAC to facilitate the maintenance of engineer details and call out schedules can be provided by either an on-line training program or by appointment.

All calls may be recorded for security and training needs

This service is available from 17:00hrs until 08:30hrs weekdays, all weekends and covering all recognised Bank Holidays as standard.

#### 11.1.1 Non-provision of Service

We ask that at all other times the company ensures cover for these calls locally as we do not normally cover demand service calls Monday to Friday 08-30hrs to 17-00hrs as these are peak traffic times for the ARC. Consideration also needs to be given to days leading up to Bank Holidays.

In the event of an emergency at the company we may offer a service on a case by case basis dependent on the circumstances. All applications for additional cover must be made to the Customer Service Manager prior to the provision being required giving at least 48 hours' notice. Normal out of hours service is **not** covered by the ARC DR/BC plans. If you wish for your service to be covered additional fees may apply.

In avoidance of doubt, additional days are charged at £100.00 per day per company.

### 11.2 Keyholder Care

Keyholder Care offers valuable peace of mind to employers and those responsible for providing a duty of care to their Keyholders when being placed in the vulnerable situation of attending site when an alarm has activated.

This protective service provides the keyholder with a set time window to attend site and return back home, with the opportunity for the keyholder to extend the time if needed. Once safely home the keyholder will close the Keyholder Care record.

If an acknowledgement of a safe return is not received, or the time window is not extended, Custodian will step in and escalate the potential risk to the keyholder's safety by alerting a chosen emergency contact.

#### 11.2.1 Value added benefits for the Company and End Users

- Keyholder Care is available to all End User Premises via their Alarm Company and is charged to the Alarm Company as an annual fee for each premises where this service is required
- This annual charge covers all the site keyholder's, existing and new, so there is no need to renew or amend the Keyholder Care details as site keyholder's change
- Available to order via TouchForms
- Campaign programme support is available to target existing base of monitored connections

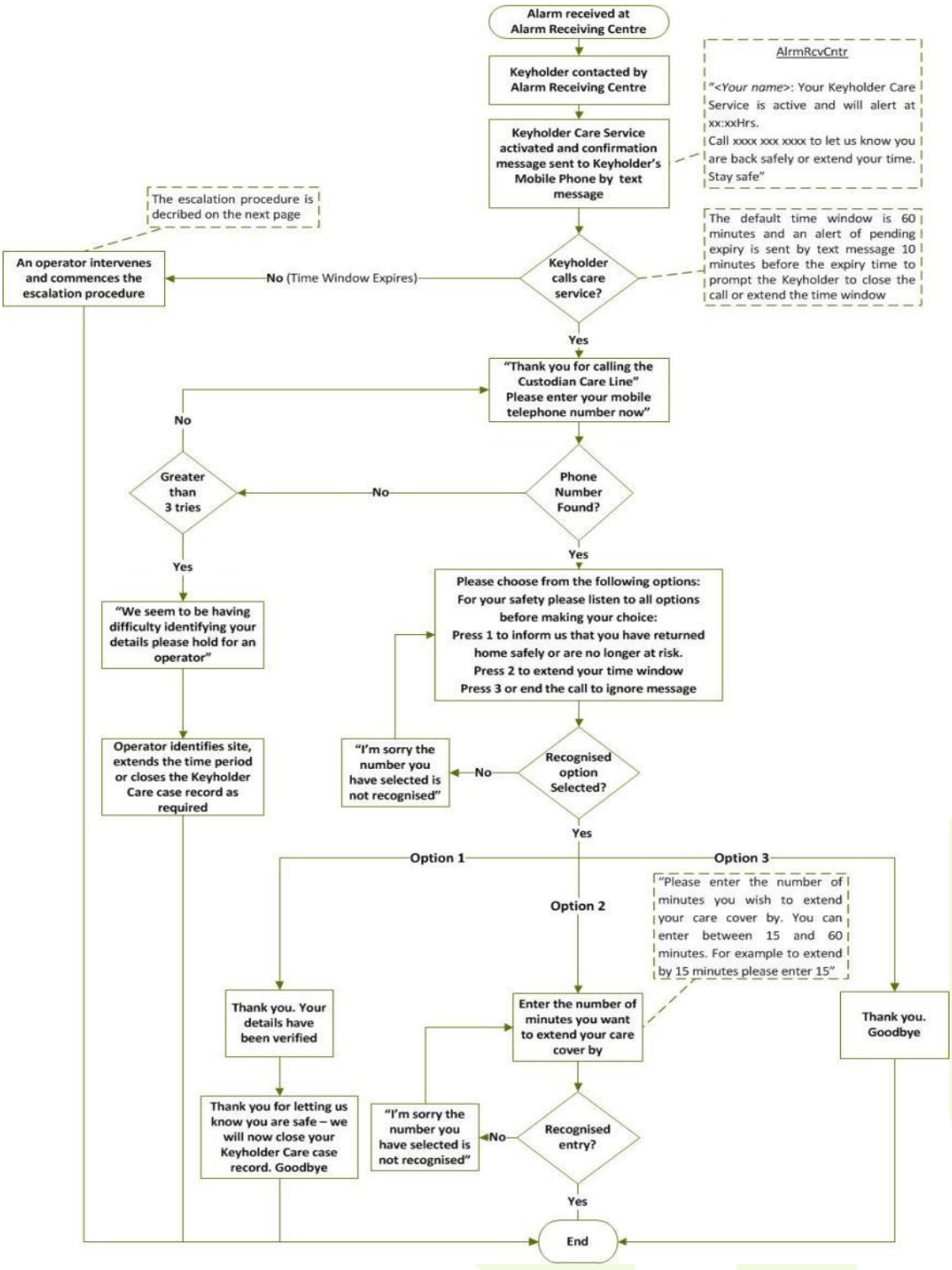
### 11.2.2 Ordering the service

The Keyholder Care service can be ordered for new and existing monitoring connections by completing the appropriate section of a New Monitoring Application Form or Keyholder Care Form within Custodian TouchForms Suite.

The Keyholder Care Escalation Keyholder is the person we should contact in the event that the Keyholder attending site, in response to an alarm activation, does not respond to Keyholder Care Assurance Messages within specified timescales.

### 11.2.3 Keyholder Care Service

The flowchart below describes the follow up actions for an alarm at premises that has subscribed to the Keyholder Care Service.



### 11.2.4 Escalation Procedure

In the event that the keyholder does not respond to the time window expiry alert, by extending the period of time or confirming they are home, the Alarm Receiving Centre Operator will proceed as described below:

#### Step 1: Call the predefined "Escalation Contact"

Notify the Escalation Contact of the alarm activation, the details of the Keyholder attending and that the Keyholder Care time window has elapsed without a response from the Keyholder.

Two attempts will be made to call the escalation contact before proceeding to step 2.

#### Step 2: Call the attending Keyholder's home telephone number, if available

If the Keyholder does not have a home number, there is no reply from their home number or it is established that the Keyholder has not returned home, then proceed to step 3.

#### Step 3: Call the "Site Keyholders"

Notify an alternative Keyholder of the alarm activation, the details of the Keyholder attending and that the Keyholder Care time window has elapsed without a response from the Keyholder.

If the escalation process is unsuccessful at the first attempt, we may make further attempts to escalate the Keyholder Care Alarm, until the call has been passed to the Escalation Contact, an alternative Keyholder or the Alarm Receiving Centre is advised the Keyholder that attended the activation is safe.

The Alarm Company will be advised in writing of all instances where we have been unable to escalate the call.

### 11.3 Lone Worker Monitoring Services

Our Nottingham Alarm Receiving Centre is inspected and approved for the monitoring of lone worker devices to BS8484, the code of practice for the provision of lone worker device services, accredited by the National Security Inspectorate.

Lone workers are vulnerable from all aspects of risk and the provision of a lone worker device may assist in summoning an emergency responder to assist when incidents occur that requires assistance from a third party.

To enable the ARC to monitor and respond to signals received from a Lone Worker Device effectively the following conditions apply:

1. The Lone Worker Device must comply with the requirements of BS8484 and the supplier must issue a certificate of conformity for the device confirming compliance with and detailing how compliance is achieved.
2. The type and model of lone worker device must have been accepted by the ARC as compatible with its alarm monitoring platform and permit alarm signals to be managed to the requirements of BS8484.
3. The ARC must be in receipt of a Monitoring Application Form for each device providing personal details of the user as defined within BS8484.
4. The ARC may only pass lone worker alarms to the emergency services where listening-in by the ARC operator or whilst in conversion with the user it is deemed by the ARC operator that an emergency response is desirable. In all cases an emergency responder other than the emergency services must be provided to assist the user in cases where an emergency service response is unavailable.

The requirements for Police attendance to lone worker devices is set out within Appendix V of the NPCC Policy.

Incident data, alarm response plans, personal details of lone workers and customer details, as provided to enable effective monitoring and response to activations received from lone worker devices, are held within our BS5979 approved ARC and across our 'quad redundant' network as described within section 2 – Technical Infrastructure. This permits monitoring to be continued at an alternative satellite configuration within the requirements of BS8484 in the event of an emergency at the normal host ARC.

### 11.4 Underwriters' Laboratories of Canada (ULC) Requirements

SMC is a part of the **APi Group, (NYSE: APG). APi Group** is **a global market-leading business service provider of safety and specialty services**. As part of SMC's international structure, our Nottingham ARC provides a disaster recovery/business continuity (DR/BC) service for the ARC in Canada. If that center is

unable to facilitate our staff to action alarm traffic, we have developed our procedures, processes & training based upon the requirements of the ULC standards, so that our operators in the UK are able to respond in accordance with the ULC standards and thus provide a seamless service to our monitored customers in Canada under DR/BC circumstances.

We recognize that providing our customers with efficient alarm response requires more than reliable technologies. The most valuable component of our monitoring service is the highly trained people who respond to and process the alarm events. SMC employs dedicated alarm center staff to ensure alarm, account data and customer follow-up are part of a consistent monitoring program.

### 11.4.1 Fire Alarm Response Performance

Fire alarm activity includes fire alarms, fire trouble alarms, fire supervisory alarms, communication failures and system tamper (transmitter cabinet tamper) alarms. Fire alarms will be dispatched to the local fire department immediately without verification. All other types of alarm instructions will not involve the fire department.

| Type of Alarm | Action taken by the ARC | KPI, Reset & Account Info |
|---|---|---|
| **UKS004**<br>**ULC FIRE ALARM** | 1. CALL FIRE DEPT TO DISPATCH<br>2. THEN CALL PREMISES TO VERIFY<br>3. IF U/A CALL KEYHOLDERS TO NOTIFY | **KPI is 30 sec to dispatch**<br>**ZONE RESET CHECK: 8 HRS**<br>**ACC: ULC-UK MONITORING STATION** |
| **UKS005**<br>**ULC FIRE TROUBLE/SUPERVISORY ALARM** | 1. CALL PREMISES TO VERIFY<br>2. IF U/A CALL KEYHOLDERS TO NOTIFY | **KPI is 5 min to notify**<br>**ZONE RESET CHECK: 12 HRS**<br>**ACC: ULC-UK MONITORING STATION** |

### 11.4.2 Burglary (Intruder) Alarm Response Performance

Burglary alarm activity includes burglary alarms, tamper alarms, communication failures & trouble alarms. All types of alarm instructions are based on the possibility that an actual crime is in progress, so verification is required. If we are unable to verify the identity of someone on site within 5 minutes from the time it has triggered, we will dispatch security.

| Type of Alarm | Action taken by the ARC | KPI, Reset & Account Info |
|---|---|---|
| **UKS001**<br>**ULC BURGLARY ALARM** | 1. CALL PREMISES TO VERIFY<br>2. IF U/A CALL SECIURITY TO DISPATCH<br>3. THEN CALL KEYHOLDERS TO NOTIFY | **KPI is 5 min to dispatch from the time of the alarm**<br>**ZONE RESET CHECK: 60 MIN**<br>**ACC: ULC-UK MONITORING STATION** |
| **UKS002**<br>**ULC BURGLARY TAMPER/TROUBLE ALARM** | 1. CALL PREMISES TO VERIFY<br>2. IF U/A CALL SECURITY TO DISPATCH<br>3. THEN CALL KEYHOLDERS TO NOTIFY | **KPI is 5 min to dispatch from the time of the alarm**<br>**ZONE RESET CHECK: 60 MIN**<br>**ACC: ULC-UK MONITORING STATION** |
| **UKS003**<br>**ULC BURGLARY COMMUNICATION FAILURE ALARM** | 1. CALL PREMISES TO VERIFY<br>2. IF U/A CALL SECURITY TO DISPATCH<br>3. THEN CALL KEYHOLDERS TO NOTIFY | **KPI is 5 min to dispatch from the time of the alarm**<br>**ZONE RESET CHECK: 60 MIN**<br>**ACC: ULC-UK MONITORING STATION** |

Where the event code states “verify” this means we must take a password when contacting this number.

IF security has been dispatched but we contact the keyholder and a cancellation is requested, we will call security back to cancel and log the call disposition code TC.

IF the zone has not restored, we will enter the appropriate zone reset pending time (as per instruction). Our Mastermind system will automatically check for a reset at the set time. If not reset, a reset pending alarm is generated.

### 11.4.3 Burglary Abort & User on Premises

"User on Premises" aborts an intruder alarm, and the alarm can be full cleared.

There are many acceptable users on premises codes that are accepted as valid for the purposes of cancelling an alarm if it is within 5 minutes of the burglary signal (a valid user ID # must be part of the signal):

1. Open signals.
2. Close signals.
3. User on Premises.

### 11.4.4 Burglary Alarm Reprioritisation

If the alarm has not been restored when full clearing, we will enter the necessary delay (as per the below)

| ACTION/ TYPE | NOTIFIED / VOICE MSG | ACTION: PC / FC | RESET REQUIRED | 1ST DELAY | 2ND DELAY | 3RD DELAY |
|---|---|---|---|---|---|---|
| **LIFE SAFETY:** Dispatched (Fire, Panic, Hold Up, Duress, Medical) | NTFD/LM | Full Clear | Yes | 1 hour | 1 hour | Full Clear |
| **LIFE SAFETY**: No Dispatch / NSA (Fire, Panic, Hold Up, Duress, Medical) | NO | Partial Clear (**951**) | Yes | 1 hour | 1 hour | Full Clear |
| **Fire Alarms Restore Required** | YES/NO | | Yes | 1 hour | 1 hour | 1 hour |
| **Burg**: Trip on **open** | | Full Clear | Yes | 30 min | 1 hour | 1 hour |
| **Burg**: Trip on **close** | | Full Clear | Yes | 15 min | 1 hour | 1 hour |
| **Burg**: Dispatched | NTFD/LM | Full Clear | Yes | 1 hour | 4 hours | 24 hours |
| **Burg**: No Dispatch | NTFD | Full Clear | Yes | 1 hour | 4 hours | 24 hours |
| **Burg**: No Dispatch | NO | Partial Clear (**951**) | No | 1 hour | 1 hour | Full Clear |
| **Burg**: No Dispatch | LM | Partial Clear (**952**) | No | 1 hour | 1 hour | Full Clear |
| **Trouble/Supervisory** (customer available) | YES | Full Clear | Yes | 4 hours | 24 hours | 24 hours |
| **Trouble/Supervisory**: (NSA: no restore) | NO | Partial Clear (**1453**) | Yes | 2 hours | 2 hours | 2 hours |
| **Trouble/Supervisory**: (NSA: no restore) | YES | Full Clear | Yes | 4 hours | 24 hours | 24 hours |
| **Trouble/Supervisory** (NSA: restored) | NO | Partial Clear (**1453**) | No | 2 hours | 2 hours | 2 hours |

Where the signal has not reset within the expected timeframe, we will call the premises and keyholders and issue CD0031. When full clearing, we set the pending alarm to 12 hours.

### 11.4.5 Communication Failure

| Type of Alarm | Action taken by the ARC | KPI, Reset & Account Info |
|---|---|---|
| **UKS006**<br>**ULC COMMUNICATION FAILURE ALARM** | 1. CALL PREMISES TO VERIFY<br>2. IF U/A CALL KEYHOLDERS TO NOTIFY | **KPI is 5 min to notify**<br>**ZONE RESET CHECK: 12 HRS**<br>**ACC: ULC-UK MONITORING STATION** |

### 11.4.6 Fail to Open/Close

| Type of Alarm | Action taken by the ARC | KPI, Reset & Account Info |
|---|---|---|
| **UKS007**<br>**ULC FAIL TO OPEN/FAIL TO CLOSE ALARM** | 1. CALL PREMISES TO VERIFY<br>2. IF U/A CALL SECURITY TO DISPATCH<br>3. THEN CALL KEYHOLDERS TO NOTIFY | **KPI is 5 min to notify**<br>**ZONE RESET CHECK: 12 HRS**<br>**ACC: ULC-UK MONITORING STATION** |

# 12. Data Protection

### 12.1 General Data Protection Regulations (GDPR)

Personal information relating to you, your employees, your customers, their authorised contacts and Keyholders will be held by our ARC on the Alarm Monitoring Computer System. Please ensure that relevant names, addresses and contact details are correct.

Information received by either post or email, including replies and forwarded copies (which may contain alterations) subsequently transmitted from the ARC are confidential and solely for the use of the intended recipient within the purpose of the original transmission. The ARC will retain this data including personal information either electronically or in hardcopy.

Telephone calls to and from our ARC are recorded for security purposes and you must ensure your employees, clients and their authorised Contacts/Keyholders are aware of this.

Personal data is retained for the periods defined within our Quality System. This is in accordance with our recognition of operating a BS5979 Category II ARC, as recognised by NSI, for the monitoring of Intruder Alarms, Fire Alarms & Lone Worker devices.

Company employees who have access to personal data, alarm system information and activation records are security screened to BS7858 as part of the company induction process and continued employment is dependent on successful security screening.

It is your responsibility to ensure that the information provided in respect of Keyholder's personal information is correct and updated, if required. In providing the Keyholders' details, you are confirming that you have authority from the individual to provide their personal information.

For further information about how we manage, store and process personal information please visit: GDPR Compliance | SMC (smc-monitoring.com)

#### 12.1.1 Holding obsolete Contacts/Keyholder details

BS5979 requires us is to hold this data for a minimum of three years after final termination.

#### 12.1.2 Disclosures required by law

Personal data will be exempt from the non-disclosure provisions when the disclosure is required by law, statute or court order, in connection with legal proceedings or for the purpose of obtaining legal advice.

### 12.2 Audio Recording for ARC Telephone Conversations

Our ARC has to comply with BS5979, therefore all inbound and outbound telephone conversations are recorded and held for a period no longer than one year. These recordings are the property of the ARC. We will only release copies of these recordings under the terms of the General Data Protection Regulations.

#### 12.2.1 Release of recording to Data Subjects

The regulations are very clear in this area and we must gain permission from all parties involved in the telephone conversation before we can release copies. It is imperative even if we release copies these are not copied or played back to a third party without our permission.

To identify and reduce time taken to recover telephone conversations it is necessary for the exact time and date of the telephone call to be provided, without this information we will be unable to fulfil the request.

The copies will only be released by e-mail, and we reserve the right to charge for the service. We do not normally make transcripts of audio conversations.

An Audio Access Request Form must be completed in full and approved by our ARC before we will release any copies of audio conversations.

#### 12.2.2 Release of audio recording for investigation of alarm incidents

Audio recording or extracts from them will be released to the Company for whom we provide the monitoring service, where required, if the content of the recording solely relates to the incident in question, i.e. intruder alarm, fire alarm or telecare monitoring service. Where the content of recordings includes personal information

and opinions unrelated to the purposes of the recording, extracts or transcripts will be released relating to the specific incident only rather than copies of the full recording.

An Audio Access Request Form must be completed in full and approved by our ARC before we will release any copies of audio conversations.

### 12.2.3 Contractual Obligations

GDPR requires that contracts between the controller (you) and the processor (SMC) includes appropriate language to record the parties duties in relation to processing data. To comply with this requirement the following clauses form part of our contract with you (this will refer to section 7):

*7.4 Personal Information Protection and Privacy*
*7.4.1 Definitions*
*7.4.1.1 "Controller" means the party that determines the purposes and means of the Processing of Personal Information. If the parties both serve as a Controller, they are Co-Controllers.*
*7.4.1.2 "Data Breach Incident" is circumstances (whether intentional, or unintentional or accidental) that involve actual or a reasonable possibility of unauthorised access to or possession of, or the loss or destruction of, Personal Information, whether ultimately confirmed or not.*
*7.4.1.3 "Data Privacy Laws" mean applicable laws and regulations relating to Personal Information protection of any country, state, or municipality with jurisdiction to regulate the activity under this Agreement.*
*7.4.1.4 "Modified Personal Information" means Personal Information that the Customer combines with other data or information, including but not limited to geolocation data, identifiers for individuals not in the Company's possession, or publicly available data. Modified Personal Information is a subset of Personal Information.*
*7.4.1.5 "Personal Information" means information and data exchanged in connection with this Agreement that is related to any identified or identifiable natural person or, to the extent of a conflict with applicable law, which is subject to any Data Privacy Laws.*
*7.4.1.6 "Processing" means any operation or set of operations performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, sharing, alignment or combination, restriction, erasure or destruction.*
*7.4.2 Compliance with Law. The Services being provided require the collection of Personal Information to function as intended. Both parties will comply with applicable Data Privacy Laws as pertaining to Personal Information Processed in connection with activity under this Agreement. If necessary, the parties will work together in good faith to make any amendments or enter into any additional agreements as may be required by a change in Data Privacy Laws.*
*7.4.3 Ownership of Personal Information. Any Personal Information contained within the Company's products or services is owned by the Company.*
*7.4.4 The Controller. Prior to providing Personal Information to the Company, the Customer is the Controller of the Personal Information and responsible for all obligations with respect to that data, including, without limitation, providing notice for the individuals for whom it provides personal information to the Company. Once the Customer has provided Personal Information to the Company, the Company and the Customer are Co-Controllers.*
*7.4.5 Shared Rights and Obligations.*
*7.4.5.1 If a party Processes Personal Information for any purpose beyond the scope of this Agreement, then that party assumes the notice obligations.*
*7.4.5.2 If the Personal Information is involved in a Data Breach Incident, the party on whose system the data was stored is responsible for any notifications and associated costs. Unless prohibited by law or a regulator with jurisdiction over a party, the party making the notification shall make reasonable efforts to coordinate with the other party to allow for input into the content of a notification before it is made.*
*7.4.5.3 While performing under this Agreement, if a party learns of any: (i) complaint or allegation indicating a violation of Data Privacy Laws regarding Personal Information; (ii) request from one or more individuals seeking to access, correct, or delete Personal Information; or (iii) inquiry or complaint from one or more individuals relation to the Processing of Personal Information, the party will exercise reasonable efforts to promptly notify the other party in writing, except to the extent prohibited by law, law enforcement, or a regulator with jurisdiction over such party. The parties shall provide reasonable commercial assistance to each other in investigating the matter, identifying the relevant information, preparing a response, implementing a remedy, and/or cooperating in the conduct of and defending against any claim, court or regulatory proceedings. The parties will take all reasonable commercial and legal steps to protect Personal Information against undue disclosure.*
*7.4.6 The Customer's Rights and Obligations.*

*7.4.6.1 If the Customer provides the Company with any Personal Information, the Customer will ensure that it has the legal right to do so. The Customer will provide notice to the individuals whose Personal Information it has provided to the Company prior to providing it to the Company. The Company has the option of providing a notice for the Customer to distribute for this purpose with the content of the notice being applicable to products and services that the Company provides under this Agreement.*
*7.4.6.2 If the Customer uses other sources of data, including without limitation geolocation information, to connect Personal Information Processed in Products or Services under this Agreement, the Customer shall have all responsibilities and obligations under Data Privacy Laws for such Modified Personal Information. The creation and Processing of Modified Personal Information shall comply with applicable law, including without limitation Data Privacy Laws.*
*7.4.6.3 If the Customer uses Personal Information or Modified Personal Information for direct marketing purposes, the Customer shall comply with, and is solely responsible for complying with, Data Privacy Laws, including any applicable obligation to conduct direct marketing only after compliant opt-in consent is explicitly obtained.*
*7.4.7 The Company's Rights and Obligations.*
*7.4.7.1 The Company may share Personal Information with the Company's service providers but only in accordance with applicable Data Privacy Laws and with appropriate protections in place.*
*7.4.7.2 The Company may store Personal Information on servers located and accessible by its parent and affiliate entities and service providers with appropriate protections in place.*
*7.4.7.3 To the extent that the Company Processes Personal Information under this Agreement, the Company will retain the Personal Information for the term of this Agreement and thereafter as may be required by this Agreement, to protect the Company's legal rights, or as may be required or permitted by law and/or audit requirements. To the extent that the Company Processes the Personal Information for purposes separate and apart from this Agreement, the Company serves as a Controller and assumes legal obligations as a Controller, including for defining the appropriate retention period.*
*7.4.8 Privacy Notice. Please review the Company's privacy notice at https://www.smc-monitoring.com/en/uk/privacy-notice/ as updated from time to time.*

### 12.2.4 What to do if you have questions or concerns

Further enquires on GDPR & our commitments to compliance should be addressed to UK_sales@smc-monitoring.com.

For independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner's Office (ICO). You can visit the ICO website at www.ico.org.uk or email them at casework@ico.org.uk

Telephone numbers for the ICO are 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

The address to write to is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

# 13. Cessation of Services

Where payment due to the Company from the Customer is over by more than one month, or where the Company has the right to termination under 6.3, SMC Service Agreement, the Company may without prejudice to its other rights on giving 7 days written notice suspend performance of any or all of the Services to the Customer for any or all of the Premises until payment has been made or the breach rectified.

# 14. ARC Suppliers

Our ARC is configured to accept alarm signals from all mainstream manufacturers and associated industry protocols. Should you require further clarification or wish to connect a new device please contact us first to check compatibility. All new devices will go through our monitoring product approval.

We do not accept the use of automated speech diallers as a form of communication path to the Alarm Receiving Centre.

Some suppliers have different terms and conditions and interpretations to reporting times. Please check with your preferred supplier.

# 15. Glossary

| Term | Definition |
|---|---|
| Alarm Condition | Condition of an alarm system, or part thereof, that results from the response of the system to the presence of a hazard. |
| Alarm Filtering | Procedure whereby signalled alarm conditions are intentionally delayed at the ARC and their status reviewed for the purpose of preventing unnecessary calls to the relevant emergency service by cancelling certain alarm conditions in line with industry standards. It is the obligation of the Company to ensure the Customer is aware that some alarm signals may be filtered. |
| Alarm Message | Message conveyed from an ARC to the relevant emergency service indicating that an alarm condition has occurred at a protected premises or providing supplementary information concerning a previously reported alarm message. |
| Alarm Receiving Centre (ARC) | Continuously manned remote centre to which information concerning the status of one or more alarm systems is reported. We trade in the UK and Ireland under the following trading name:<br><br>Security Monitoring Centres Limited<br><br>Therefore any reference to the ARC in this document may be referring to either name. |
| Alarm Signal | Signal which, upon being received at an ARC or other remote location, identifies a signalled alarm condition. |
| Alarm Transmission Equipment (ATE) | Defines equipment that transmits signals to the ARC. |
| Agency or/and Agencies | An emergency service for example Police, Fire, Ambulance, Keyholding Service, etc. |
| Audibly Confirmed | Status in which an incident has been confirmed by an ARC Operator at a remote location (normally an ARC), having interpreted audio information transmitted from the protected premises, has made a decision that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred. |
| Confirmed Alarm | Condition that follows after two independent actions or signals have been generated from an audible, visual, or sequential source confirming there is a high probability that a genuine alarm has occurred. |
| Control and Indicating Equipment (CIE) | Equipment for receiving, processing, controlling, indicating and initiating the onward transmission of information. |
| Commissioned System | A statement used by the ARC to facilitate the connection process to ensure all the critical data is present and the signalling system has been tested to the ARC and commissioned by the attending engineer. |
| Company or Companies | Organisation that provides service and maintenance for alarm systems or who pays for the monitoring service for example Alarm Company, National Account or End User. |
| Contact / Keyholder | A representative of the protected premises with authority to make changes to the ARC response to signalled alarm conditions and/or attend the protected premises in response to signalled alarm conditions**.** |
| Control Panel Unit (CPU) | The user interface for the alarm system. |
| Customer / End-user | Person or organisation utilising the services of an Alarm Company. |
| Disposition Reason | Reason for alarm activity |
| Early to Open (ETO) | A system that is unset prior to the scheduled opening time |
| Global System for Mobile Communications (GSM) | A network used by some signalling devices to transport alarm conditions to the ARC. |
| General Packet Radio Service (GPRS) | A network used by some signalling devices to transport alarm conditions to the ARC. |
| False Alert (FA) | Signalled alarm condition that without having been extended to the relevant emergency service is regarded by the ARC as cancelled either by an open or abort, if programmed, or mis-operation validated by the customer / end-user quoting their authorised password. |

| Term | Definition |
|---|---|
| History | A table of event history, including open/close signal, alarm conditions, ARC actions and service call out logs (where applicable). |
| Hold-up Alarm System (HAS) | An alarm system that incorporates Hold-up/Panic Alarm Devices |
| Intruder Alarm System (IAS) | An alarm system that is designed to detect intrusion. |
| In Service | A site/system placed 'in service' has reached a status where alarm conditions received will be processed by the ARC. |
| Internet Protocol (IP) | A network used by some signalling devices to transport alarm conditions to the ARC. |
| Local Area Network (LAN) | Local Network available to support communication suppliers to transport alarm conditions to the ARC. |
| Last Alarm Condition | The last time an alarm condition was communicated to the ARC from the protected premises. |
| Late Restoral Alarm Condition (LRAC) | An alarm condition that has not restored to its quiescent state within a predefined period. |
| Late to Close (LTC) | A system that remains unset after the scheduled closing time. |
| Line Failure/ No Response / Line Fault / Path Failure | A break in the communications link between the protected premises and the ARC. |
| MasterMind | The Alarm Receiving Centre monitoring software. |
| Mis-operation signal | Signal that is definitely and unambiguously identifiable at the ARC as indicating to the ARC that the alarm system has mis-operated and therefore that the alarm signal is to be filtered out and not extended to the relevant emergency service. |
| Monitoring Centre Transceiver (MCT) | Alarm transmission equipment. |
| On test/off test | A mechanism for an authorised person/engineer to ask the ARC to ignore alarm conditions during a period of time not exceeding 24hours. |
| Operator / Agent | A member of the ARC team who may be involved in dispatch of alarm conditions or administrative procedures. |
| Order | The result of sending a monitoring application form to the ARC. |
| Out of hours (OOH) | Out of normal working hours |
| Out of service (OOS) | Alarm signals received for a site/system that has been placed out of service will be ignored until such time that instructions are received to reinstate the monitoring service. |
| Personal Attack/Hold Up Alarm | A manually operated device at the protected premises, normally requiring a double input to be activated |
| Paknet - Vodaphone | A network used by some signalling devices to transport alarm conditions to the ARC. |
| Polling | A process used to determine if the signalling system is still in place and operational. |
| Polling Server (PSV) | The server that is polling the communication device. |
| PIN (Personal Identification number)/ Password | A unique identifier for the customer / end-user / engineer to identify themselves to the ARC. |
| Protected Premises | The part of a building to which protection is afforded by an alarm system. |
| Public Switch Telephone Network (PSTN) | A network used by some signalling devices to transport alarm conditions to the ARC. |
| Receiving Centre Transceiver (RCT) | Alarm transmission equipment. |
| Remote Restore / Remote Reset (RR) | A process where the customer/end-user calls a Restore Management Centre, normally the ARC, to obtain a code to facilitate resetting of the alarm system. |
| Response Agreement | Set of instructions agreed between the ARC and the Company or End User as to the actions to be taken in the event of an alarm signal being received by the ARC. |
| Restore | An alarm condition that has restored to its normal state. |
| Router | Multilayer switching device |
| Sequentially Confirmed | Status in which confirmation emanates from two or more independent sensors, detectors, hold-up devices and/or processors, which are so configured that there |

| Term | Definition |
|---|---|
| | is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred. |
| Signalled Alarm Condition | State of monitoring equipment at an ARC (or other remote location) that indicates intrusion, attempted intrusion or unauthorised interference has occurred at the protected premises or is likely to occur. |
| Signalling | The transmission of an alarm condition from the protected premises to a remote location. |
| Signalling Devices | Transmission equipment for sending alarm conditions to the ARC. |
| Site/Protected Premises | The location where the alarm is installed. |
| Status | This identifies the status of a zone and if it requires restoring. |
| Supervised Premises Transceiver (SPT) | Alarm transmission equipment |
| Suspend Monitoring | A method to ask the ARC to ignore alarm conditions for more than 24hrs, billing continues during this period. |
| System | The alarm system installed at the protected premises. |
| Unconfirmed Alarm | A single alarm activation, i.e. a signal that has not been designated as audibly, visually or sequentially confirmed |
| Unset / Set or Open / Close or Disarm / Armed | Varying terms used to describe if an Intruder Alarm System (IAS) is set or unset. |
| URN & URN Status (Permit & Permit Dispatch Status**)** | The Unique Reference Number (URN) issued by the Police or Fire Authorities and the status, for example Level 1 (On Response) authorities may attend or Level 3 withdrawn (Off response) authorities may not attend. |
| User | Person authorised to operate an alarm system. |
| Visually Confirmed | Status which is confirmed by an ARC Operator being at a remote location (normally an ARC), after having interpreted a visual image transmitted from the protected premises, has made a decision that there is a high probability that a genuine intrusion, or a genuine attempted intrusion, has occurred. |
| Wide Area Network (WAN) | External Network for communication suppliers to transport alarm conditions to the ARC. |
| Zones (Channels) | Segmentation of the alarm system to enable differing alarm conditions to be identified and signalled to the ARC. |

# 16. Certification

Certificate Number 2259/ARC-G

GOLD

National Security Inspectorate

Certificate of Approval

Security Monitoring Centres Ltd
Trading as
Custodian Monitoring
Crocus Street, The Meadows, Nottingham, Nottinghamshire, NG2 3EJ

Has been assessed by the National Security Inspectorate (NSI) for the

ARC Gold Approval Scheme

and satisfies the requirements of:

Scope

RVRC Monitoring BS 8418 Detector Activated CCTV Systems and other CCTV Systems used in Security Applications, BS 5979 Security Monitoring (Cat II), Monitoring of Lone Worker Devices, Monitoring of Intruder Alarms, Monitoring of Fire Alarms

Alarm Receiving Centre based
NOTTINGHAM

Demonstrating compliance with

BS 5979:2007 - Remote Monitoring Centres, BS 7858:2019 - Screening of Individuals, BS 8418:2015 - Detector-activated Video Surveillance Systems (CCTV), BS 8484:2022 – Lone Worker for services provided, BS 9518:2021 - Processing of Alarm Signals, BS EN ISO 9001:2015 - Quality Management Systems, NSI SSQS 102 - Alarm Receiving Centre

| | |
|---|---|
| Original Issue Date | 28/02/1992 |
| Effective Date | 01/04/2024 |
| Valid Until | 31/03/2027 |

Authorised by Richard Fogelman
NSI Chief Executive

UKAS CERTIFICATION 0142 UKAS INSPECTION 0142

Further clarification regarding the Scope of this Certificate may be obtained from: NSI, Sentinel House, 5 Reform Road, Maidenhead SL6 8BY UK | www.nsi.org.uk
The certificate of approval remains the property of NSI and must be returned on demand. Approval is conditional upon the Approved company continuing to comply with NSI Regulations and Criteria.

Security Industry Authority

Certificate of Approval

This is to certify that

**Security Monitoring Centres Limited**

**t/a SMC Vision**

| Start date | End date |
|---|---|
| 1 April 2024 | 31 March 2025 |

Has met the requirements of the
Security Industry Authority's
Approved Contractor Scheme

APPROVED CONTRACTOR

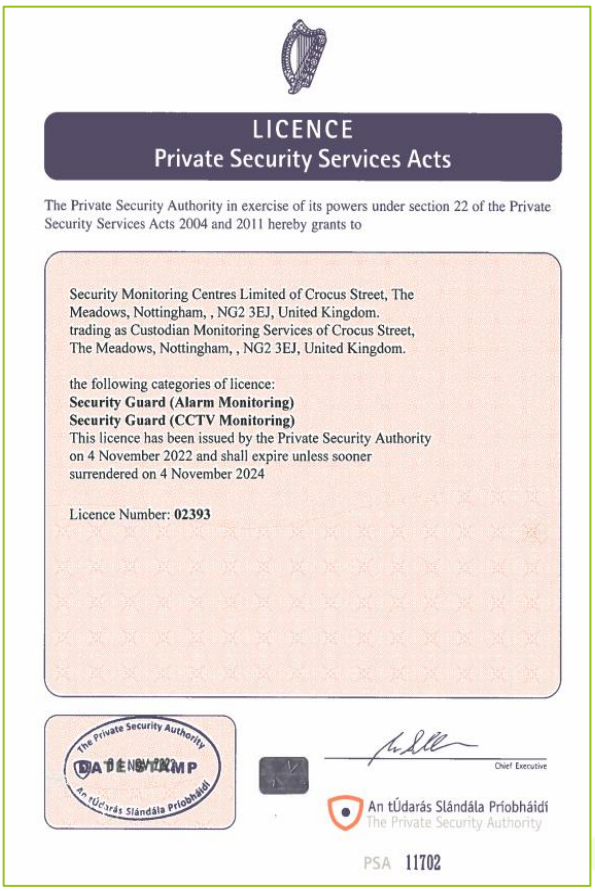
In achieving approved contractor status, the SIA has approved the above organisation for the activities of:

**Security Guarding**

Assessing Body:

**NSI**

Authentication and further detail is available on the SIA Approved Contractor Register:
www.sia.homeoffice.gov.uk/roac



LICENCE
Private Security Services Acts

The Private Security Authority in exercise of its powers under section 22 of the Private Security Services Acts 2004 and 2011 hereby grants to

Security Monitoring Centres Limited of Crocus Street, The Meadows, Nottingham, , NG2 3EJ, United Kingdom.
trading as Custodian Monitoring Services of Crocus Street, The Meadows, Nottingham, , NG2 3EJ, United Kingdom.

the following categories of licence:
**Security Guard (Alarm Monitoring)**
**Security Guard (CCTV Monitoring)**
This licence has been issued by the Private Security Authority on 4 November 2022 and shall expire unless sooner surrendered on 4 November 2024

Licence Number: **02393**

The Private Security Authority An tÚdarás Slándála Príobháidí

Chief Executive

An tÚdarás Slándála Príobháidí
The Private Security Authority

PSA 11702

CerticCS

Certificate of approval

This certifies that

**SECURITY MONITORING CENTRES LTD**
Trading as
**CUSTODIAN MONITORING**
Crocus Street
The Meadows
Nottingham
Nottinghamshire NG2 3EJ

Has been assessed and satisfies the requirements of

**CERTICCS ARC**

**for the scope(s):**

Security Guard (Alarm Monitoring)
Security Guard (Video Surveillance Systems (CCTV) Monitoring)

Demonstrating compliance with:
I.S. 228:1997 - Monitoring Centres for Intruder Alarm Systems
PSA 33:2014 - CCTV Monitoring & Alarm
SR 25 - ARC Alarm Handling Procedures
for services provided
at
ALARM RECEIVING CENTRE – NOTTINGHAM

**The above company is approved by CerticCS**

**25/06/2009**
Original Issue date

**01/04/2023**
Effective date

**01/04/2023**
Certification Cycle Start Date

**Chief Executive**

**31/03/2025**
Expiry date

**24087**
Approval Number

Date Printed 14 March 2023
**Further clarification regarding the Scope of this Certificate may be obtained from CerticCS, Sentinel House, Reform Road, Maidenhead SL6 8BY, UK**

CerticCS telephone 01628 764888

The independent certification body for Ireland www.nsi.org.uk

This certificate remains the property of CerticCS and must be returned on demand.
Approval is conditional upon the Approved Company continuing to satisfy all the rules and other requirements applicable to this CerticCS scheme.
CerticCS is a trading division of Insight Certification Ltd.

Party Site No.: 3488105
Expires: 31-Dec-2024

## CERTIFICATE OF COMPLIANCE

**THIS IS TO CERTIFY** that the Alarm / Service Company identified below is included by - UL Solutions (UL) in its UL Product iQ directories as eligible to use the UL Listing Mark in connection with Certificated Systems. The only evidence of compliance with UL's requirements is the issuance of a UL Certificate for the System and the Certificate is active under UL's Certificate Verification Service. This Certificate does not apply in any way to the communication channel between the protected property and any facility that monitors signals from the protected property.

**Listed Service From: NOTTINGHAM**

**Alarm / Service Company: (3488105)**
CHUBB FIRE & SECURITY CANADA CORPORATION
THE MEADOWS
CROCUS STREET
NOTTINGHAM NG2 3EJ UNITED KINGDOM

**The Alarm / Service Company is Listed in the following Certificate Service Categories:**

| File | Vol No. | CCN | Listing Category |
|---|---|---|---|
| S6837 | 21 | DAYIC | Fire Protective Signalling (Full Service) |
| BP7497 | 21 | CPVXC | Commercial Intrusion (Full Service) |
| BP7493 | 21 | CRXXC | Financial Intrusion (Full Service) |

***** THIS CERTIFICATE EXPIRES ON 31-DEC-24 *****
"LOOK FOR THE UL ALARM / SYSTEM CERTIFICATE"

ELITE ASSURED

CHAS

common assessment standard

CERTIFICATE OF ACCREDITATION

This is to certify that

**Security Monitoring Centres (SMC)**

**Membership No.: 0005072**
**Common Assessment Standard**

has been awarded certification after demonstrating compliance with the CHAS standards in line with the requirements of the Common Assessment Standard and UK H&S Legislation. An onsite audit has been conducted, validating the submission with a wide range of current legislation in relation to policy, procedures and arrangements.

Ian McKinnon
Managing Director

CHAS ACCREDITATION ELITE ASSURED

MEMBERSHIP VALID UNTIL 03 NOVEMBER 2024
CERTIFICATE VALID UNTIL* 06 MARCH 2025
*Certificate is only valid when accompanied with an active membership

0345 521 9111
CHAS.co.uk

The information on this certificate is correct at the time of issue. To confirm the validity of a contractor, please visit https://portal.chas.co.uk

CYBER ESSENTIALS

# CERTIFICATE OF ASSURANCE

Security Monitoring Centres Limited

Shadsworth Road Blackburn BB1 2PR

**COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME**

NAME OF ASSESSOR : Shruthi Hasmkal (PGI)

CERTIFICATE NUMBER : 24b56c80-2739-46bf-9617-6370385beb83

PROFILE VERSION : 3.1 (Montpellier)

SCOPE : Whole Organisation

DATE OF CERTIFICATION : 2024-06-19

RECERTIFICATION DUE : 2025-06-19

SCAN QR CODE TO VERIFY THE AUTHENTICITY OF THIS CERTIFICATE

CERTIFICATION MARK

CYBER ESSENTIALS CERTIFIED

CERTIFICATION BODY

PGI

CYBER ESSENTIALS PARTNER

IASME CONSORTIUM

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against a cyber attack.

# Part 2 - SMC VISION

# 1. Introduction

This section has been prepared exclusively for SMC Vision customers. It sets out essential information regarding the services provided to Alarm Companies 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 section 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 are always available to assist you further.

Information provided within this booklet is in accordance with BS8418 'Installation and remote monitoring of detector activated CCTV systems – Code of Practice, and BS5979 'Code of practice for remote centres receiving signals from security systems.

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

- BS8418 Installation and remote monitoring of detector activated CCTV systems - Code of practice
- BS5979 Remote centres receiving signals from fire and security systems – Code of practice
- BS9518 Processing of alarm signals by an alarm receiving centre Code of practice
- BS7958 Closed circuit television (CCTV) – Management and operation – Code of practice
- BS7992 Code of practice for exterior deterrent systems
- BS EN 50131-1 Alarm systems – Intrusion and Hold-up system – Part 1: System requirements
- BS EN 50132-7 Alarm Systems – CCTV surveillance systems for use in security applications – Part 7: Application Guidelines
- BS8243 Installation and configuration of intruder and hold-up alarms designated to generate confirmed alarm conditions - Code of practice
- BS EN 50518 Monitoring and Alarm Receiving Centre
- BS8473 Intruder and hold-up alarm systems - Management of false alarms – Code of practice
- BS10008 Evidential weight and legal admissibility - specification
- The Criminal Procedure and Investigations Act
- General Data Protection Regulations (GDPR)
- The Human Rights Act
- SIA – Security Industry Authority

The above references were correct at the time of going to print. SMC Vision cannot be held responsible for changes of standards not contained within this document.

The SMC Vision Remote Video Response centre conforms to both BS5979 for Category II Alarm Receiving Centres and BS8418 for the Installation and Remote Monitoring of Detector Activated CCTV Systems. Our Quality Systems are recognised by the NSI for the monitoring of CCTV Systems, Intruder, Hold-up and Fire Alarms.

All SMC Vision operatives are licensed under the SIA scheme for CCTV Public Space Surveillance (PSS). SMC Vision operates the SIA Approved Contractor Scheme for all new employees and those undergoing Licence Training and Application. For further details visit www.sia.homeoffice.gov.uk.

The Nottingham SMC is registered with the Private Security Authority in Ireland for the monitoring of Intruder Alarms and CCTV Alarm Systems. We hold approval through CertisCS for the monitoring of Intruder Alarms in the Republic of Ireland.

# 2. General Information

### 2.1 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: Where a URN has not been provided by the Alarm Company for a CCTV system, SMC Vision will not normally pass alarm incidents to Police Authorities who require a URN.

It is the responsibility of the maintaining company to ensure that any change in status of a URN that will affect SMC Vision's response to alarm incidents is notified, in writing, to SMC Vision immediately.

SMC Vision 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
- 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.

Where the type of alarm system does not require a URN, should we be requested and where allowed we will endeavour to contact the Police via alternative means.

### 2.2 Alarm Company Security Codes

Certain information exchanged with an Alarm Company 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.

### 2.3 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 30 characters of his/her own choice. The Alarm Receiving Centre 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.

### 2.4 Connection Forms

SMC Vision complies with all relevant BS and EN Quality standards. As you would expect from a conforming Security Company, data accuracy is essential, SMC Vision therefore ask that the relevant documentation supports all new connections to the monitoring centre; this should also include amendments to existing systems.

If you have any queries relating to the completion of an SMC Vision Connection Form, please contact our Customer Support Team on 0844 879 1007 who will be pleased to advise you.

### 2.5 Instructing the Alarm Receiving Centre

Due to the security nature of instructions and the implications of an accurate response, we would ask that all instructions from Alarm Companies are made in writing on the appropriate form. Where End Users instructions cannot be forwarded via the Alarm Company they should be received on company headed paper. Data changes can also be made via TOUCH (for further information please contact our Customer Support Team on 0844 879 1007).

Emergency changes relating to Contacts, Passwords, Site and Contact Telephone Numbers or Open/Closing Times (monitored), can be accepted directly from End Users, provided they are registered Contacts and hold legitimate passwords.

**IMPORTANT NOTE: Audit Liability**
The management of data is the most critical process within SMC Vision and requires the highest level of management control by both the Alarm Company and SMC Vision.

We strongly advise that at least once per year you carry out a critical data audit, i.e. telephone numbers, URN, Contacts, etc.

SMC Vision 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 Alarm Company
- Where instructions have been submitted on non-SMC Vision recognised forms
- Where the Alarm Company has not monitored the receipt of SMC Vision data change acknowledgements or has not audited received acknowledgements for correctness
- Where incorrect entries have been made on TOUCH

For all non-CCTV alarms please refer to Section 1 of this booklet.

# 3. CCTV Overview

### 3.1 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 control rooms.

Over recent years technical development has made remote monitoring more viable. SMC Vision has invested significantly to establish our Remote Video Response Centre which can provide a best in class service to its customers.

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. Monitoring personnel need to be confident that activations only originate from genuine intruder activity, therefore wrongly specified systems offered to clients as a cost saving alternative to traditional guarding solutions severely damage the reputation of installers and SMC's.

### 3.2 CCTV Surveillance System

A typical CCTV surveillance system comprises the following component equipment:

- Site Cameras
- Camera control equipment
- Detection Equipment
- Communications equipment / Digital Video Recorder / Network Video Recorder
- System controls
- Audio interface
- Router

### 3.3 System Configuration

Details of the site installation should be provided to SMC Vision using a CCTV Connection Form (SMCFMVIS005) and Site Plan (SMCPLVIS011).

### 3.4 Definitions and Abbreviations

**Detector Activated Monitoring**: Incident based monitoring arising from automatic detection of activity in a restricted area causing the CCTV system to alert SMC Vision of unwanted activity on the protected site. A trained operator is then able to review alarm images from the system and carry out a predefined response plan.

*It should be noted that owing to the wide range of technology available, exact operational protocols of SMC Vision supported equipment should be confirmed with SMC Vision prior to final specification of any system by the installation / maintaining company.*

**Cameras**: Units containing an imaging device that produce a video signal from an optical image.

**Camera Control Equipment**: Transmission and receiving devices for controlling remotely, such features as pan / tilt and lens functions.

**Closed Period**: The time between the system being set and unset at the protected site. This could be overnight or for a weekend, could change according to site type and should always exclude periods where it may be reasonable for the General Public to have access to the site. Special consideration should be given to vehicle dealerships.

**Communicator Audio Interface**: A device enabling one-or two-way audio communications. *Excludes audio for access control purposes.

**Communicator**: A device enabling digital and analogue communication signals to be passed via telephone, Internet or radio links to and from an SMC.

**Digital or Network Video Recorder (DVR or NVR)**: Devices installed at site and the remote monitoring station for recording video images from site cameras.

**IP:** Internet Protocol

**Pre-commissioning Tests:** Tests carried out on site and prior to achieving connectivity with SMC Vision, to demonstrate the effectiveness of the installed system and its suitability for acceptance by SMC Vision.

**PTZ alarm driven presets**: Settings of a fully functional camera unit, controlled locally, enabling the device to react to pre-determined alarm positions on site.

**Recorder:** Equipment to provide either intermittent or continuous recording of video images.

**Remote Video Response Centre:** A manned operation capable of receiving multiple concurrent CCTV images from remote locations for the purpose of interacting with the site(s) to provide security and related services.

**Sensors:** A device installed to detect change in background conditions. This may be in the form of Passive Infrared detectors (PIR), Active Beams or Video Analytics

**Server:** A device installed at SMC Vision enabling processing of alarm signals transmitted from a site installation.

**System Control:** A device within a secure environment enabling all equipment installed at site to be functionally controlled.

**System Control (Remote):** Equipment permitting an SMC to control specific functions of a site installation.

**Walk Test:** A system test carried out between the on-site engineer and SMC Vision, where connectivity is initiated from site following activation of on-site detection equipment.

### 3.5 CCTV Monitoring

Effective and reliable CCTV surveillance can only be achieved if the fundamental criteria of system design have been addressed and all potentially influencing factors carefully considered.

Successful detection of intruders is dependent on minimising false / unwanted activations and the overall operational efficiency of SMC Vision. Monitoring can be provided by:

- A contracted monitoring service with installing company using installing company's own RVRC
- A contracted monitoring service through installer with a RVRC operated by a subcontractor
- A contracted monitoring service direct with independent RVRC

All three categories can generally be defined as Remote Video Response Centres.

### 3.6 Installation Standards

Detection systems should be installed to BS8418 and the appropriate parts of BS EN 50131, this standard provides the requirements for intrusion systems and in addition for systems that provide an exterior deterrent 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
- Audio challenges
- Monitoring and response
- Identification Resolution (personal features, vehicle number plates, where possible, regulatory conditions

apply)
- Recognition (personal features, vehicle number plates, where possible, regulatory conditions apply)
- Compliant signal recording

Considerations

- Open / closed site
- Lighting levels
- Obstacles
- Bright lights / Glare
- Reflections
- Direct sunlight
- Prevailing environment
- Site management
- Air conditioning outlets
- Detection overspill

Options / Features

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

The rapid rate of development precludes prescriptive recommendations; however it is possible to design efficient cost effective systems if the essential criteria are identified in advance.

### 3.7 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;

- Ensure that sensors strictly relate to visible horizons. Sensor activations that cannot be related to a definitive cause will inevitably lead to "False Alarm" comments; identification difficulties debase the entire installation efficiency.
- Restrict sensor range to covering confines of the enclosed site, ensuring that activations are not triggered by movement from adjoining footpaths or roadways, care should be taken to ensure cameras do not overlook public areas. If detection is triggered by passers-by or traffic outside the designed installation boundary remote intervention will be initiated occupying valuable receiving equipment and human resources.
- Sensor fields should ensure that unauthorised movements cross the beam rather than entering the field head on.
- The negative effects of the rising and setting sun both on CCTV images 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 and paired should be considered.
- Multiple detectors connected to a single PTZ device that automatically drive cameras to preset locations should be individually connected to the transmission alarm Input and be identified by the CCTV system. Cameras should be programmed to return to a reference field of view linked to an appropriate sensor following completion of an event.
- 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.
- 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.
- Entry/exit routes should be viewed by fixed cameras or a PTZ camera with its parked position viewing the entry/exit route.
- Detectors should only cause activations within the specified field of view of associated cameras.
- 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.

- Lighting should not be positioned to directly face cameras and where timers control lighting these should be changed to and from British Summer Time and should not create an alarm where video analytics is employed.
- 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.
- 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.
- The system should send continuous video images whilst under surveillance by SMC Vision.
- Video loss, tampers, line failure, power failure and failure of CCTV system within a set condition should be signalled to SMC Vision and should be utilised as laid down in the relevant BS. Such signals should be sounded locally during an unset condition
- 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 SMC Vision may not be suitable for systems that are required to meet BS8418.
- Where sites are classified as vehicle dealerships and are open to the public for viewing - The system should remain isolated in those areas designated as 'open' until 10pm BST and 7PM GMT. SMC Vision reserve the right to isolate areas outside those times.
- Systems that generate alarms through legitimate entry and exit from the premises may be isolated without prior notification.

### 3.8 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 General Data Protection Regulations (GDPR) 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 and residential areas

The primary requirements of BS7958 are;

#### 3.8.1 Objectives and Policies

The objectives of the CCTV system should be documented in writing and an example of a typical policy statement is provided in appendix C.

#### 3.8.2 Documented Procedures

Documented procedures should, for operation of the CCTV system, typically cover:

- Organisational responsibilities in connection with the system
- Administration
- Staffing and training
- Communication
- Documentation
- Control room operations, where applicable
- Access and security screening, including remote access
- Data handling and disclosure
- Observation and incident protocol
- Administration of recorded material registers
- Maintenance and faults
- Investigation, complaints, non- disclosure and disciplinary measures
- Periodic review and reporting
- Standard forms

#### 3.8.3 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 General Data Protection Regulations.

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.

### 3.8.4 Other operational considerations

The following recommendations are considered good practice and provide a resume 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 and is the responsibility of the site manager. Facilities for remote checks exist and can be arranged by separate negotiation. Unless contracted to provide such a service the reporting of failed lighting should not be assumed as the responsibility of SMC Vision.
- The owner of the CCTV scheme should comply with a selection of recruitment requirements of BS7499 static site guarding and mobile patrol procedures code of practice.

Signage is normally provided by your CCTV Installer/Maintainer.

## 3.9 System Specification

Integrated communication, receiving, remote control and signal recording interfaces are available. SMC Vision preferred systems and respective operational protocols for these technologies 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 position and ideally should be limited to 50M maximum per preset.

Telemetry and transmission protocols should always be verified with SMC Vision prior to specification.

## 3.10 Monitoring Suspension & Reinstatement

### 3.10.1 Suspension

A method used by SMC Vision to ignore all alarm conditions for a period of more than 24 hours. All instructions must be confirmed in writing but may be accepted over the telephone from an Authorised Company Representative or Engineer:

- Billing will continue during the suspension period.
- SMC Vision will not allow suspensions with an end date.
- The Company must review the suspended systems weekly to ensure the suspension is still required.

### 3.10.2 Re-instatement

The instruction to reinstate a suspended system is normally required in writing but may be accepted over the telephone from an Authorised Company Representative or Engineer.

# 4. CCTV Monitoring Contracts

### 4.1 Overview

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

1. Standard Terms and Conditions (Not applicable to intruder monitoring)
2. CCTV Contract
3. Local Agreement System specification comprising;
   - Insurance Requirements
   - Connection Documentation
   - Customer Requirements
   - System Record
   - Police details / URN
4. SMC Vision Monitoring Quotation

### 4.2 Responsibilities

SMC Vision 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 NPCC requirements.

Where monitoring is carried out for an Alarm Company, the alarm company is responsible for ensuring that all applications for connection into SMC Vision are covered under the current standard CCTV Monitoring agreement before applying to make the system live. The alarm company must also ensure that installations meet with the client and industry standard requirements. The alarm company must notify SMC Vision of any changes to the monitored installation in writing, failure to notify of such changes may result in inappropriate action being taken in response to an alarm event.

Direct End Users are responsible for ensuring that all applications for connection into SMC Vision are covered by a current standard CCTV monitoring agreement before applying to make the system live. The End User must also ensure that installations meet with industry requirements and that SMC Vision is notified of any changes to the monitored installation in writing, failure to notify of such changes may result in inappropriate action being taken in response to an alarm event.

### 4.3 Contract Documents

Standard Monitoring Agreement: A Standard Monitoring agreement (SMCFMVIS003) details the particular conditions applied to CCTV monitoring arrangements.

Local Agreement: This document is specific to the installation and forms the basis of an agreement between the end user and installation / maintaining company.

Details of the site installation, response plan in the event of alarm activity and equipment installed should be confirmed on the CCTV Connection Form (SMCFMVIS005).

The layout of the site and camera / sensor fields of view shall be identified on the Site Plan (SMCPLVIS011).

System Records identifying SMC Vision interpretation of the Connection Form, Site Plan and any standing instructions will be retained by SMC Vision, together with a Commissioning Form (SMCFMVIS009) indicating the outcome of the system commissioning.

# 5. Connection of CCTV Systems

### 5.1 How to organise a connection

Monitoring connections can only be made live if contractual arrangements have been formalised.

If you wish to make a connection into SMC Vision you need to carry out the following:

- If you do not already have a monitoring agreement with SMC Vision contact the SMC Vision Customer Service team on 0844 879 1007 to arrange for the relevant documentation to be forwarded for signature.
- Advise SMC Vision of the intended connection date.
- Confirm that the installation complies with BS8418, an appropriate code of practice adopted by regulatory bodies such as the NSI & SSAIB 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 SMC Vision.
- Complete CCTV Connection Forms.
- 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 SMC Vision.

On receipt of your notification SMC Vision will set up a system record file with the basic details which will allow you to carry out any necessary preliminary system testing. Please allow 48 hours for processing of connection data before attending site to conduct system commissioning. (Under exceptional circumstances will be endeavour to process sites in a shorter time frame providing resources allow).

### 5.2 Preliminary Testing

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

Please note that SMC Vision will not retain records of preliminary testing.

### 5.3 Making a System Live

Before each system is made live SMC Vision 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 SMC Vision to process incoming signals.

System commissioning can only take place between 9am and 4pm Monday to Friday (excluding Bank Holidays) unless prior arrangements have been made. NB. additional costs may be incurred for out of hours commissioning work.

SMC Vision are 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 Section 6 of this handbook. The Commissioning Record together with the Connection Form and Site Plan constitutes the specific schedule to the Monitoring Contract.

SMC Vision reserve the right to apply a 30 minute variation to CCTV schedules should it become apparent that excessive false positive alarms are being generated as a result of non-adherence to agreed schedules. Any such amendments by SMC Vision will be confirmed to the installer via email.

# 6. Commissioning of Installations

### 6.1 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 connection to SMC Vision is made from the site and each camera / sensor is activated and critical assessment made of the monitored images in both day and night conditions.

### 6.2 Commissioning Procedure

Prior to commencing commissioning a system, SMC Vision will prepare a system record file from the CCTV Connection Form, Site Plan and the CCTV Site Commissioning Record Form.

The installer must carry out pre-commissioning tests and make appropriate adjustment / 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.

### 6.3 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 SMC Vision, ensuring that they are correlated with the appropriate camera, source location display should also be tested if available
   - Testing all cameras linking to SMC Vision
   - 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 will be stored for finalised camera views and PTZ presets. (If preset changes are required at any time SMC Vision must be notified)
   - Testing of audio links
   - All daytime tests should be carried out whilst the system is armed from site. Tests where connectivity is achieved by connecting from SMC Vision to site will not be accepted as this fails to prove connectivity on alarm and verify alignment of detector fields of view with those of the CCTV camera
   - Storage of reference images

2. Night-time Testing
   - Night checks to assess quality of image resolution & supplementary lighting (where applicable).
   - Storage of reference images

3. Seven Day Environmental Soak Testing
   - During this period the system remains under review to permit evaluation of the effects of environmental influences as laid down in BS8418
   - Where isolations occur owing to unwanted alarms or false alarms with no defined cause the 7-day soak test will be ceased and restarted after notification of rectification to SMC Vision by the installer.

### 6.4 Acceptance of System

Acceptance of a system for monitoring is the sole discretion of SMC Vision.

Certification will not be issued to any system that has not completed the full 7 day soak test cycle.

**Notes:**

1. Only after successful completion of the commissioning process does SMC Vision contractual obligation commence. SMC Vision will confirm acceptance by returning an acceptance certificate to the customer. Any limitations regarding the operation of the system by SMC Vision will be identified and documented on a soak test commissioning report.
2. Where commissioning is unsuccessful within the initial 7-day period SMC Vision will advise the Installer of the actions required. It will remain the responsibility of the installer to effect remedial repairs and the commissioning process is completed successfully.

# 7. Incident Handling Options

### 7.1 Overview

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

Monitoring of CCTV installations has numerous permutations, SMC Vision have standard monitoring procedures covering each major option available. The main options are:

- Linked with approved intruder alarm and/or hold-up alarm
- Not linked with intruder or unapproved system
- Linked with audio challenge
- Guard Tours
- Customer action / notification Instructions
- Notification of emergency authorities for compliant systems
- Notification of keyholders
- Prescribed action on failure to achieve contact
- Communication line Integrity checks

### 7.2 Monitoring Options

#### 7.2.1 Linked with approved intruder alarm and/or hold-up alarm

It is anticipated that where a PD6662 and BS8243 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 by the Installation / maintaining company, from the relevant police authority.

- On receipt of an activation SMC Vision will connect to the site to ascertain a reason for the activation.
- If there is reasonable cause to believe that the activation is the result of unauthorised interference with the security of the site or genuine activation of hold-up alarm, the operator will advise the police stating that they have received a visually verified alarm, quoting the Unique Reference Number if allocated. Associated keyholders will be contacted in conjunction with the relevant emergency services; keyholders are required to attend where requested and are responsible for their safe transportation to and from the protected site.
- Where keyholders are unavailable or will not attend, in the case of BS8418 systems issued with a URN, the police will be updated that keyholders are not attending. In the case of a non-approved system the police will not be called and the incident closed.
- Where it is not possible to determine whether a suspected presence is authorised, SMC Vision will follow the response plan provided by the customer.
- In instances where no reason can be determined for the activation the incident will be updated on the event log and action taken in accordance with the associated response plan.

If a CCTV system is to be used to supplement a PD6662/BS8243 Intruder Alarm system as confirmation technology, the signalling path should conform to PD6662/BS8243 requirements.

#### 7.2.2 Not linked with approved intruder alarm, hold-up alarm or unapproved system

Where the installation is not linked to a police approved intruder alarm and / or the CCTV system is not compliant with PD6662/BS8243, the system will be considered simply as an aid to determine whether security at the site has been breached.

- On receipt of an activation SMC Vision will connect to the site by the pre-described means to ascertain a reason for the activation.
- If it is clear that a malicious incursion has occurred at the site, SMC Vision will attempt to notify (where specified and detailed on the site response plan) the relevant Emergency Services. Should the call not be accepted by the Emergency Services the primary contact will be informed.
- Where it is not possible to determine whether a suspected presence is authorised, SMC Vision will follow the response plan provided by the customer.
- In instances where no reason can be determined for the activation the incident will be updated on the event log as a "false alarm".
- Where the initial incident has no visible cause the first alarm may subsequently have multiple activations

from the same camera in a queue requiring a response. In this situation whilst SMC Vision will endeavour to view all alarms, the assumption will be made that these subsequent alarms will contain no visible activity, as it will be assumed that the detection and associated CCTV camera are directly aligned. SMC Vision will therefore not guarantee a response to activity received after the initial event.

### 7.2.3 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. SMC Vision 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.

### 7.2.4 Guard Tours

Integrated camera position presets can be programmed to enable predetermined guard tours to be carried out.

If there is inferior picture quality or interference with field of view where appropriate the relevant parties will be advised.

### 7.2.5 Access Control

It is not practicable to monitor closed sites with personnel present. Where authorised site access control is a feature of the installation, it is implicit that the access control system will automatically disarm the system on first entry and re-arm on last exit. SMC Vision 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 SMC Vision.

Live testing of the system to SMC Vision without prior notification is not accepted. Failure to formally place a system on test with SMC Vision prior to carrying out system checks could result in loss of Police response. Additional charges may also be made to the Installation / Maintenance Company.

# 8. CCTV Incident Monitoring

### 8.1 Active Incident Handling

#### 8.1.1 Alarm Images

In the event of a detected Incident at the remote site the system should be capable of one of the following:

- Transmitting a sequence of stored images captured during the incident. SMC Vision will view these stored alarm images before reviewing live pictures to determine the likely cause of the event
- Transmitting alarm information via text* format allowing SMC Vision to retrieve images from the site before reviewing stored and live images to determine the likely cause of the event

**Special note***: **Consideration should be given by the Installation / Maintenance Company as to the exact operation of the CCTV transmission types supported by SMC, as owing to the disparate nature of the equipment operational processes and procedures will differ greatly. Full details are available upon request and should always be ratified prior to final system design and specification.***

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” (consideration should be given to section 7 of this document). Subsequent events arising from the same alarm may not be viewed by an operator where the initial alarm is deemed as ‘nothing seen’. Where a site is still in its commissioning process only the initial alarm will be viewed, as the stability and reliability of the system or part of cannot be guaranteed at this point. Please note SMC Vision will not automatically guard tour a site where nothing is seen on the alarm Image. It should also be noted that where a definitive cause of the alarm is apparent any further activity should provide additional alerts to SMC Vision highlighting an increased risk on site.

#### 8.1.2 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 SMC Vision will advise the site contact or keyholders of the problem. Video loss alarms are not able to be passed to the Police unless supported by visually confirmed alarm images. Please refer to section 2.1 for confirmation of Police response.

Video loss signals should be reported and receive action locally whilst the system is unset.

### 8.2 Response Plan

Specific instructions must be in place confirming the action you require SMC Vision to carry out on receipt of an activation from the site. It is essential that these instructions are worded briefly, clearly and represent realistic actions, recognising that these instructions have to be transcribed to the SMC Vision 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 SMC Vision. Email to data-changes@smc-monitoring.com or by TOUCH. Amendments should be kept to a minimum and be made during normal working hours where possible.

### 8.3 Police Intervention

Police Intervention is determined in accordance with the prevailing NPCC policy.

#### 8.3.1 URN Issuing

The issue of Unique Reference Numbers to enable Police Response to a protected site is governed by the prevailing NPCC 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.

#### 8.3.2 Risk Assessment

In determining Police Response to a protected site the level of risk to a site must be ascertained. In the event that persons are seen but no actual sign of malicious act is detected, where appropriate, SMC Vision will contact the site / Keyholder to request further instructions.

### 8.4 Calling Contacts/Keyholders

There should be a minimum of two Contacts/Keyholders available 24 hours a day for seven days per week with 1 contact being a mobile telephone number as a minimum requirement, in accordance with NPCC requirements. A 24-hour keyholding service can be utilised as one of the two required Contacts/Keyholders. To maintain operational efficiencies and to avoid extended delays in alarm response we recommend that there is a maximum of four Keyholders. Each Keyholder should have transport available and should reside within 20 minutes travelling distance of the protected premises.

- We will ring for approximately 30 seconds before terminating the call during the day (0700 -1859 hours) and proceeding through the contact list
- We will ring for approximately 60 seconds before terminating the call during the night (0000 -0659 and 1900 - 2359 hours) and proceeding through the contact list
- In the event of all Keyholders being unavailable, SMC Vision may take appropriate action to ensure that other systems remain unaffected by the consequence of incorrect Keyholder data or unobtainable keyholders
- In the event that SMC Vision has been unable to speak to an authorised Keyholder, notification will be sent to the contracted party, where and as soon as possible, normally next working day, stating that all Keyholders were unavailable
- Messages will not normally be left on Answer phones for security reasons
- Once a legitimate Keyholder has been contacted, the incident will be closed. Should a Keyholder decline to attend the premises it will be their responsibility to contact another authorised Keyholder
- It is 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 travelling to site
- The announcement of the SMC Vision telephone number to telephones that display ‘Caller I.D.’ cannot be guaranteed

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

#### 8.4.1 Automation of Incident Response

To improve efficiency and to provide a quicker response to alarm incidents we may use an automated process for dialling Keyholders, this results in the SMC Vision Agent only becoming involved once a successful call is made at the time the keyholder answers the telephone.

Please see Appendix B for details of the Operator Assist process.

### 8.5 AI Analytic Alarm Filtering

SMC Vision reserve the right to implement AI/Analytic Alarm filtering packages to identify and control unwanted and false CCTV signal traffic. These services are provided by external suppliers and managed by SMC Vision. Within the AI/Analytic Alarm filtering package SMC Vision reserves the right to adjust and amend internal settings where appropriate.

### 8.6 Proactive CCTV Maintenance Check

SMC Vision provides a proactive CCTV maintenance check to verify the health and status of the on-site DVR/NVR. Standard default checks are –

- System connection
- Camera failure
- Disk Recording
- Recoding Duration
- Time accuracy
- Image integrity

Notification of these checks are sent via email and can be accessed by the provided web portal.

# 9. False Alarms

## 9.1 General

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

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

## 9.2 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 SMC Vision to direct resources to priority monitoring tasks.

| **Technology Type** | **Zone Isolation** | | | | **System Isolation** |
|---|---|---|---|---|---|
| | **3 FA in 1hr per zone (1hr omission)** | | **A further 3 FA within any subsequent hour of the following 24hr period per zone (Permanent isolation)** | | **3 FA in 1hr (System suspended)** |
| | Local Omission | SMC Omission | Local Isolation | SMC Isolation | MAS only |
| Xtralis ISDN | ✓ | | ✓ | | |
| Xtralis ADSL | ✓ | | ✓ | | |
| IMMIX compatible | | ✓ | | ✓ | |
| RSI | | | | | ✓ |

Key ✓ = Compatible
**FA** = False Alarms

Note: Legacy Remguard customers' false alarm management will remain controlled from within the Aquila unit. New systems installed using Hikvision will be control as the table above.

## 9.3 Disablement Procedure

Where an installation generates excessive numbers of activations SMC Vision will either:

- Notify the end user and/or installer and request that the problem is addressed and/or advise that the alarm input will be omitted. The omission can be for one hour (first offence) or permanent isolation where a device has exceeded 6 alarms in any 24 hour period.

The Camera/Sensor Omission/Isolation assessment criteria are as follows;

- Any camera/sensor generating more than three false alarms in any one hour period will be omitted for a period of one hour, where possible the subscriber (or representative) will be advised. After one hour the camera/sensor will be returned to active status
- If the installation continues to communicate false activations, where possible, the subscriber (or representative) will be notified of our intention to isolate the affected camera/sensor until the problem is rectified
- Formal notification will be made in the event of malfunctioning equipment or suspected environmental effects. Where contact details have not been provided or are out of dates notifications cannot be guaranteed
- The notification confirms actions taken and should also be used to confirm 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 may be made for each activation in excess of the agreed contractual amount
- Where systems use AI/Analytic filtering, after an input is isolated due to false activations, a maintenance

walk test may not be required. In this instance, please contact SMC Vision who will advise next steps.

### 9.3.1 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 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
- Where possible an alarm company or subscriber has been contacted and advised of the situation, SMC Vision turn the camera/sensor off; and all details and actions have been logged.
- Confirmation of disarming is emailed to the alarm company by using a SMC Vision fault report form

**Note:** Following camera/sensor disablement it is the responsibility of the Alarm Company to confirm instructions to SMC Vision to re-enable cameras/sensors. Re-enabling devices can only be carried out during those hours pre-determined for the commissioning of new systems. If after re-enablement a device continues to transmit false alarms, the device may be isolated immediately and in the absence of the above process, fault notification will be provided. Re-commissioning should be carried out using the form SMCFMVIS039.

### 9.4 Testing Conditions

It is imperative if a system is being tested by a customer/engineer that it is placed 'on test' prior to testing. This will ensure that whilst testing, an alarm event is not passed to an ARC Agent for action and the creation of a call to the keyholder(s) and or the emergency services in error.

Non-adherence to the testing processes below has a detrimental effect on response times for genuine events; the ARC is unable to differentiate between genuine and non-genuine signals received. Should incidents of this nature occur the ARC is under no obligation to investigate instances where testing protocols have not been followed.

Pre-booking a test with the ARC for a time in the future could be a security risk and should also be discouraged.

Should a system require to be placed on test for longer than 24 hours a request for suspension of service must be made in writing as described within section 3.10.

If multiple tests are carried out by engineers and customers, care must be taken to ensure the tester does not override the other party's tests.

# 10. Remote Access to Site

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

### 10.1 Preventative Maintenance

A planned programme of preventive maintenance and system checks prescribed in NCP104 (or equivalent) and BS 8418 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 an SMC Vision 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 out 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" carried out in conjunction with SMC Vision whilst the system is armed from the remote site. Service levels should be agreed in writing prior to commencement of service. Some or all checks may be carried out automatically using smart software.

### 10.2 Corrective Maintenance

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

### 10.3 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 SMC Vision preferably using a Site Commissioning Record Form. In the event of any fault being identified a record of the findings will be communicated to the Alarm Company.

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

#### 10.3.1 Engineer Tests

Engineers should advise SMC Vision of their arrival on site and instruct that the system should be placed on test. Engineer must demonstrate authorisation by password etc.

Service Engineers will need to be registered as an authorised engineer with SMC Vision. Engineers 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. Ideally the test should follow the pre-arranged sequence.

On completion of the test SMC Vision and the onsite 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 or requested by the customer, new reference images will be stored to reflect changes.

Engineers should advise SMC Vision of their Intention to leave site & instruct that the site should be taken off test.

#### 10.3.2 Customer Walk Test

Customers may undertake a walk test of the system by prior arrangement with SMC Vision. Site Representative should identify themselves by name with a relevant authorisation password and notify of their intention to test the system.

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

The records should be agreed and include site, engineer/site representative, password, day, date & extent of test.

# 11. Records and Reports

### 11.1 Overview
The principal records retained by SMC Vision are;

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

### 11.2 Detail of Records
#### 11.2.1 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. All events are time and date stamped. The maintainer/system owner should ensure accuracy of the time and dates on all equipment at the remote location.

#### 11.2.2 CCTV Images
All images received at SMC Vision are recorded on digital video recording equipment. These images are stored in digital form to hard drive. Video records are retained for a period of 31 days and may be available subject to data release requirements of section 14.

#### 11.2.3 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 disablement and enablement.

#### 11.2.4 Voice Communications
All inbound and outbound telephone calls are recorded for training and security purposes.

#### 11.2.5 Notifications
Notifications of site, keyholders, emergency authorities and alarm companies are logged, and where applicable allocated incident numbers recorded.

#### 11.2.6 Disablements
Operators have the facility to carry out disablement/enablement of cameras and sensors where these are causing problems that are affecting the overall efficiency of SMC Vision. Where disablement is necessary the appropriate notification should be made as detailed in section 9 of this document.

#### 11.2.7 System Records and Changes to Instructions
Connection details are retained and changes to monitoring instructions are logged.

#### 11.2.8 Activation Reports
Activation logs and associated actions taken are retained for 3 years. Summaries are forwarded daily to Alarm Companies. Any changes to contact details should be notified in writing to SMC Vision.

### 11.3 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 perceived abnormal observation during a routine check on an installation the subscriber will be advised verbally.
- Camera/sensor disablement notifications: Confirming disarming of cameras/sensors when fault conditions have occurred.
- Video Image Copies: Where appropriate copies of video images received at SMC Vision can be provided. Bespoke reporting options are available upon request.
- All reasonable requests will not be subject to an administration charge however, where the request is deemed to be excessive or manifestly unfounded, SMC reserve the right to charge a “reasonable fee” to cover the administrative costs of complying with such requests.

# 12. Quality Checks

The following quality checks can be pro-actively carried out by SMC Vision and are subject to contractual and service level agreement:

### 12.1 Weekly system health checks

SMC Vision will, where possible, or where specific contract arrangements have been made, remotely access the system; each camera view will be accessed to ensure that a clear image quality can be obtained in line with the reference images stored. SMC Vision will notify the customer by exception by email if a fault is detected.

### 12.2 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 by email to the maintaining company advising them of the nature of the problem and requesting remedial action be taken.

### 12.3 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. keyholder no longer valid) a fixed format notification will be issued to the maintaining company by email requesting the supply of the missing data.

# 13. Service Levels

### 13.1 Incident Response Time

SMC Vision categorise systems according to the standard that they are accredited to, namely;

- Type A: BS8418 - Alarm signal from systems certified to BS8418 will be prioritised.
- Type B: These systems are certified against an appropriate code of practice adopted by regulatory bodies such as the NSI & SSAIB – For these systems SMC Vision will endeavour to action alarms in accordance with BS5979.

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 reduction in service levels.

### 13.2 Local System Fault Reporting

When faults are detected on the system, in addition to any reporting at the time of the incident customers will be notified by email the next working day.

### 13.3 Telephone Response

Wherever possible the monitoring station will ensure that:

- 80% of calls are answered within 15 seconds

### 13.4 Incident Investigation

#### 13.4.1 Incident Investigation Requests

Alarm Company 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

All requests should be sent using form number SMCFMVIS022

#### 13.4.2 Incident Investigation Reports

Our response will provide:

- Verbal acknowledgement and interim response within 24 hours
- Written response including video Image review with accompanying data normally within three working days (subject to approval by the companies' legal representative).

#### 13.4.3 Video Record Retention

Recordings covering periods under investigation will be quarantined for six months from date of receipt of incident investigation request unless advised in writing and acknowledged by SMC Vision.

### 13.5 Customer Complaints

Complaints received in writing will be dealt with as follows: Alarm Companies should contact SMC Vision with information regarding the complaint.

SMC Vision provides an interim verbal report within twenty-four hours and a full written report normally within three working days, subject to the conditions detailed above. All communications will be sent to the primary customer unless formal written instructions are given to the contrary.

Verbal complaints will not be responded to in any predefined process.

### 13.6 Event Reporting
All events recorded within a closed period will be reported where possible by email to the customer's nominated contact during the next working day.

### 13.7 New Site Connection
A new site will be set up for commissioning within 24 hours of receipt of the completed documentation. Details of the documentation required can be found in sections 4 and 5 of this booklet.

### 13.8 Adverse Weather & Unforeseen Circumstances
### 13.8.1 Operations Team
Our ARC maintains operating levels to meet normal fluctuations of alarm signal traffic and have contingency plans in place should alarm signals reach unacceptable levels. In adverse and unforeseen circumstances, notably through severe weather conditions, extended power / network failures or National/Global Emergencies including epidemics or pandemics where signals received may exceed the number of operators available, the alarm queue will be managed;

- Our operators will prioritize the following high priority signals: Telecare, Fire Alarms, PA, Lone Worker and confirmed intruder where a valid URN is in place. All other signals will be automated which means that text* messages will be sent to keyholders informing them of any activations outside of the above priority signals.
- In the case of CCTV, subject to the volume of activations at any given time we will introduce a revised amount of allowable false alarms to a maximum of three in an hour (false and unwanted). Once the system has reached this limit it will be isolated and a fault report sent to the Company until the cause is resolved.

Important Actions to note:

1. Please ensure keyholders are made aware of those activations as detailed above which will be notified in text* format.
2. Please check all keyholder details to establish which do not have a mobile number and provide us with one for those that don't. Updates should be made via the TOUCH portal. If you use a keyholding company this may require you to agree with your keyholding company for them to provide a mobile phone number for this purpose.

### 13.8.2 Customer Support Team
In line with the contingency plans above, the Customer support team could be in a position whereby remote working capabilities are mobilised. This will enable the team to continue to access our systems for inputting changes, updates and ordering of signaling devices. Unfortunately, due to our customer support teams working remotely from home, waiting times on our phone lines could be longer than normal (including for data amendments), and we need your help to prioritize the most important calls and requests. Therefore, we would ask you to please use TOUCH to make simple changes and updates to your keyholder details. Please only contact us if you are unable to use TOUCH.

**If you do not have TOUCH, please register at [www.smc-monitoring.com](http://www.smc-monitoring.com)**

### 13.8.3 In the Event of Centre Closure
We will endeavor to activate the following support:

- Remote working for customer support team;
- Operations will only action the following critical signals: Telecare, Fire Alarms, PA, Lone Worker and confirmed intruder.
- In the case of CCTV, subject to the volume of activations at any given time we will introduce a revised amount of allowable false alarms to a maximum of three in an hour (false and unwanted). Once the system has reached this limit it will be isolated and a fault report sent to the Company until the cause is resolved.
- Non-essential services such as out-of-hours call handling may not be available.

# 14. Data Protection

Please refer to Appendix A for details of the SMC Privacy Notice

# 15. Video Verified Systems

CCTV system installed to permit verification of conventional intruder alarms signals prior to passing alarms to the Police as 'video verified' must be installed and maintained to the requirements of PD6662 and BS8243.

For remote verification purposes the key elements of BS8243 are summarised below:

| | |
|---|---|
| Field of view: | Imaging devices should be sited to avoid light sources that interfere with viewing by the ARC operator. The field of view should be illuminated so that the ARC receives a clear image.<br><br>An imaging device should view the whole area of coverage of any accompanying detector and any area associated with a Hold-up Device.<br><br>After an alarm condition there should be a minimum of three images transmitted to the ARC, one image at the time of the alarm condition. Subsequently, there should be two more images within 5 seconds of the alarm condition. |
| Sequential Confirmation: | Intruder alarm systems equipped with visual confirmation of intruder detection should also be configured to generate sequentially confirmed alarms.<br>Note: For systems installed to meet BS8243:2021, the previous provision for all intruder and hold-up alarm systems (I&HAS) to include sequential confirmation is now optional. |
| Restricted Access: | It should only be possible to view images from a supervised premises in a remote location, following receipt of an alarm condition. Once the ARC has viewed images and then logged off, unless otherwise agreed with the client, it should not be possible for the ARC to view images again until a further alarm condition is received at the ARC. |
| Alarm Designation: | As soon as the ARC reaches a decision, according to agreed procedures, that the images emanating from the supervised premises are consistent with intrusion at the supervised premises, the alarm signal should be designated as being a visually confirmed alarm signal.<br>If images are inconclusive the alarm signal should not be designated as being a visually confirmed and the Control and Indicating Equipment (CIE) at the supervised premises should subsequently send a sequentially confirmed alarm signal to the ARC should a second alarm activation occur that meets the criteria of sequentially confirmed within the confirmation time.<br><br>ARC actions in the event of visually confirmed alarms and alarms that are designated by the ARC as false will be as agreed with the client. |

# 16. Cessation of Services

Where payment due to the Company from the Customer is over by more than one month, or where the Company has the right to termination under 6.3, SMC Service Agreement, the Company may without prejudice to its other rights on giving 7 days written notice suspend performance of any or all of the Services to the Customer for any or all of the Premises until payment has been made or the breach rectified.

# Appendix A – SMC Privacy Notice ("Notice")

This Privacy Notice addresses how Security Monitoring Centres Limited, Chubb House, Shadsworth Road, Blackburn BB1 2PR ("SMC") may collect and process personal information from you, separate and apart from its websites and mobile applications. The privacy notice for the SMC website is available on that particular website.

SMC interacts with individuals in a variety of ways: employees of SMC customers, contact persons of SMC customers and end users of SMC products and services. To enable these interactions, SMC is collecting and processing personal information. SMC has implemented technical, organizational, administrative, and physical measures to safeguard any personal information SMC may process. As this Notice is intended to cover a variety of situations, some information in this Notice may not apply to you.

This Notice may be modified from time to time without prior notice. Please review this Notice on a regular basis for any changes. The effective date of the current version appears at the end of this Notice.

### What personal information might SMC collect?

The personal information that SMC collects is subject to applicable legal and contractual requirements. Because this Notice covers a wide variety of situations, there may be data elements listed here that do not apply to your specific situation. Please contact SMC if you have any questions.

### Type of personal information

- Name and salutation (such as Mr. or Mrs.)
- Emergency contact information
- Work contact information, including telephone number, email address, mailing address, and work location
- Home address, personal email address and home telephone number, including personal mobile telephone number
- Information about an individual's employer, including company name(s), company location(s), company address(es), and country of incorporation
- Job title, department and job function
- Visitor information, including the time of arrival and departure, date, name visitor, name company, location of visits, information regarding the vehicle for parking purposes, information required for a badge (which may include a photograph), visitor's signature and information necessary to maintain visitor logs and screening.
- Payment and invoice-related information, including identification and bank account numbers
- Information collected through a voluntary survey or promotional campaign
- Record of any incident that occurs while on SMC premises
- Information that may be collected as part of the execution of the contract, such as time and attendance data, badge information, photographs, audio, video, or geolocation data used for a particular role or assignment
- Government-issued identification numbers (in whole or in part), such as a tax identification number, VAT number
- Information provided to facilitate a service or request assistance, such as product use or problem information
- Information required to process a claim or any information that a person chooses to include in a document that is part of a legal proceeding involving SMC
- Live video images when responding to alarm triggering events, and audio recordings. Live video images and telephone recordings.
- In case of IP connections with the SMC alarm center: IP addresses are stored.
- In case of SMC's Tracking & Tracing services: location is stored.
- In case of SMC's video services: username / password, IP addresses and video images are stored.
- For the Alarm Processing System: the log book is stored (and in some cases access information).
- In case of monitoring of (ex) prisoners: criminal background info might be stored.
- Information regarding health and injuries, such as disability, sickness, accident related info, and other related information that may be part of video images, recorded conversations, and actions linked to responding to alarm triggering events
- Medical information and history; next of kin/emergency contact details; medication details; GP details; security passwords and access codes; events history.

## How might SMC use the personal information it collects?

### Purpose

- Conducting regular business operations, including designing and developing products, managing an Enterprise Resource Planning (ERP) system, sending invoices and collecting payment, providing payment, and providing goods and services to customers, which may include sharing limited personal information with customers or other business partners
- Providing requested products and services, which may include use of geolocation for certain applications in a known and transparent manner. Providing details and information about other products and services that can be supplied.
- Managing communications and notices
- Managing physical security, including access controls and security, facility access and safety, and disaster preparedness
- Responding to alarm triggering events
- Overseeing location tracking, duration, and other telematics of certain SMC assets and applications for management of services provided, security, safety, and efficiency. Ensuring compliance with import, export, and other international trade controls, including screening for sanctioned or restricted countries or parties
- Performing audits and compliance reviews to ensure compliance with applicable policy, regulation, and law
- Conducting and managing internal and external investigations, including Legal, Global Ethics & Compliance, and International Trade Compliance reviews and any resulting disclosures to government agencies
- Evaluating and reporting conflicts of interest
- Addressing environmental, health, and safety issues, including injury and damage claims
- Prosecuting and defending claims in litigation, arbitration, administrative, or regulatory proceedings, including but not limited to pre-dispute activity, evidence collection, discovery, litigation holds and e-discovery efforts
- Responding to law enforcement and other government inquiries
- Administering of marketing, contract, joint ventures, and other business efforts, including without limitation invoice and payment processing, project management, and customer surveys and promotions
- Designing, selling, producing, and improving products
- Providing customer service and support
- As required or expressly authorized by applicable law or regulation
- For training of SMC employees and quality purposes of SMC products and services
  - − The Alarm Processing System
  - − For alarm processing of incoming alarms (log book is stored and in some cases access information)
  - − National Response whereby a security agency is getting orders from SMC (e.g. by checking on the location in case of an alarm) and whereby the name, address and telephone number of the customer can be provided
- Video platforms
  - − To be able to assess the video images
  - − In case of an alarm, SMC employees and the local police can watch “live” video images
  - − For the contract administration and invoicing
- Tracking & Tracing application
  - − For locating
- Teleservice application
  - − For handling incoming messages at the teleservices
- Archive
  - − For storage of the customer’s file

<u>Responding to situations involving a risk of health or safety, including an emergency and accident</u>

## With whom might SMC share the information it collects?

SMC will not sell or otherwise share your personal information outside SMC, except to:

- APi Group, (SMC’s ultimate parent company) with a registered office at 1100 Old Highway 8 NW, New Brighton, Minnesota, United States. SMC and its businesses shall not transfer Personal Information from one country to another or from one legal entity to another, unless properly supported by law and an adequately secured technical and contractual process, such as an intra-group data processing and transfer agreement.
- APi group companies to enable them to offer you products or services, to include but not limited to Mentor Business Services Limited.

- service providers SMC has retained to perform services on SMC behalf. SMC will only share your personal information with service providers with whom SMC has signed a processing agreement except as necessary to perform services on SMC behalf or to comply with legal requirements, including but not limited to in response to a legitimate legal request from law enforcement authorities or other government regulators;
- investigate suspected or actual illegal activity;
- prevent physical harm or financial loss; or
- Urgent Community Response/Emergency Services
- support the sale or transfer of all or a portion of SMC business or assets, including through bankruptcy.

### Where does SMC store your personal information?

SMC stores your Personal Information in United Kingdom, Ireland and Europe. Personal Information may also be stored worldwide, however there are Data Transfer Agreements in place should the information be shared. Further, for customer and visitor screening, the control is carried out via an automated database of one of SMC's service providers currently located in the United States. SMC has signed a data transfer agreement with the service provider to guarantee the protection of the data.

### How long does SMC retain Personal Information?

SMC retains personal information for the length of time required to fulfil the purpose for which it was originally collected and for any additional period as required by applicable law or regulation, court, administrative or arbitration proceedings, or audit requirements.

### What choices do you have about how SMC uses your personal information?

SMC will use your personal information for executing its contractual obligations towards its customers and business partners.

You will always have a choice about whether SMC uses your personal information for direct marketing purposes. If you have provided SMC with your personal information and would now like to request that it is no longer used for marketing purposes, please contact UK_sales@smc-monitoring.com.

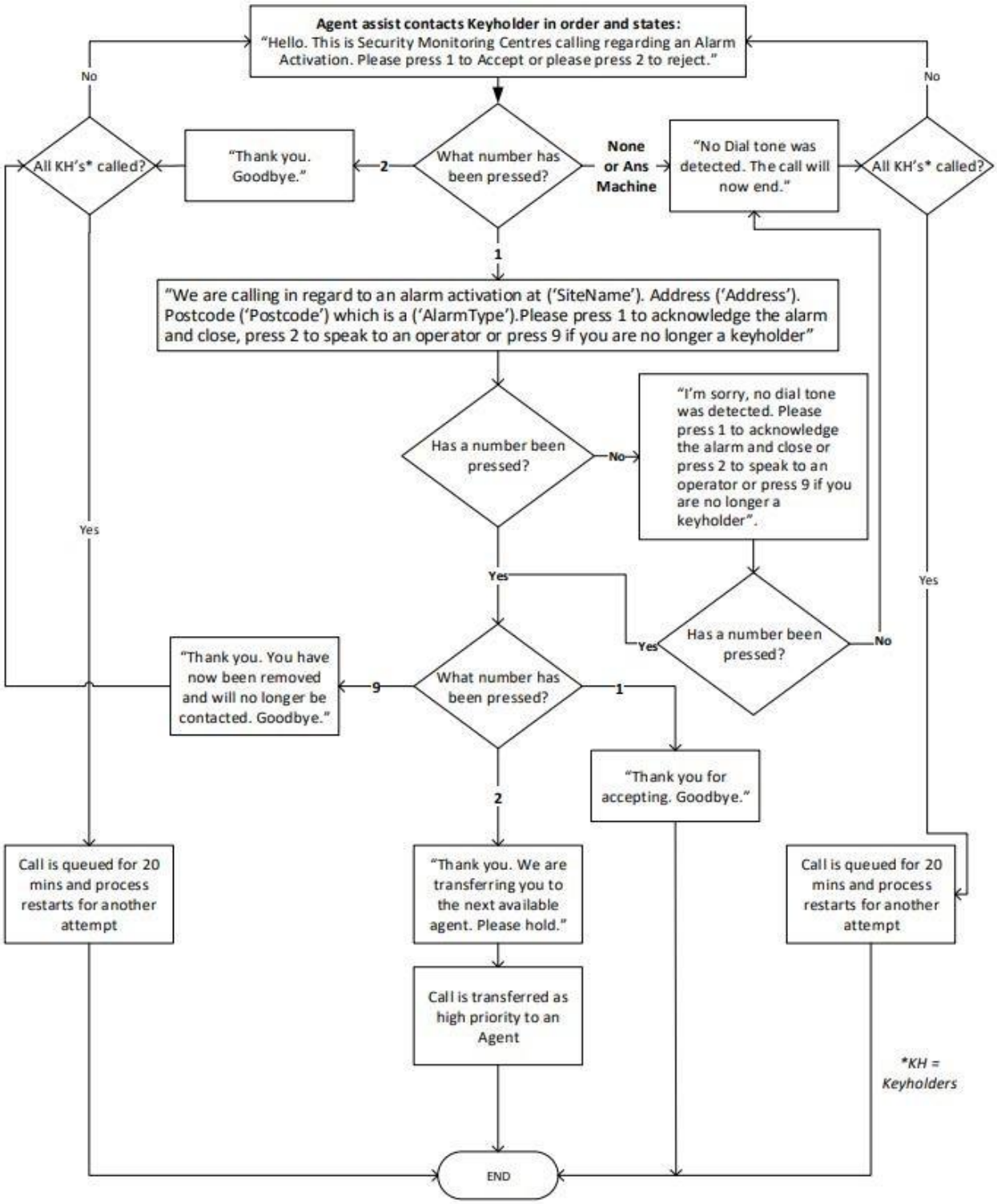
You have the right to lodge a complaint with the Information Commissioner's Office. You also have the right to withdraw consent, to request access to and correction or erasure of your personal information, seek restrictions on or object to the processing of certain personal information, and seek data portability under certain circumstances. To contact SMC regarding the above, please email UK_sales@smc-monitoring.com

### How can you contact SMC?

If you wish to access, correct or update your personal information, or if you have questions about SMC's privacy practices in general or a complaint, please email UK_sales@smc-monitoring.com

Last Updated: 30th August 2024

# Appendix B – Operator Assist Process



# Appendix C – Typical 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. Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; Video recorders designated record only; Video recorders designated play-back only, digital recorders, Magnetic tape erasers; Public information signs; Recording tapes>.

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
- assist in the identification of persons visiting the premises

The system will not be used for any purpose not stated above.

<Insert where applicable – At all times where the public have a right of entry the premises are designated as a “public place” as defined under the Public Order Act, 1986 and the requirements of the Surveillance Camera Code of Practice apply.>

### 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 Security Monitoring Centres at the address below;

Security Monitoring Centres, Crocus Street, The Meadows, Nottingham, NG2 3EJ.  Tel: 0844 879 1911

Access is restricted to authorised members of senior management, 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 General Data Protection Regulations; 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 Company ensures that all staff are fully briefed and trained in respect of their responsibilities from the use of CCTV and that any contracted personnel are licensed under the SIA Public Space Surveillance Guidelines. Training in the requirements of the General Data Protection Regulations 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 system log up to and including its final erasure and disposal. The Log is kept secure and access to it is only available to authorised members of staff.

All recordings remain the property of <Company Name> until disposal and destruction.

### 8.0 Access to recordings

Access to recordings will be restricted to those staff that need access in accordance with the purposes of the system.

### 8.1 Access to recordings by third parties

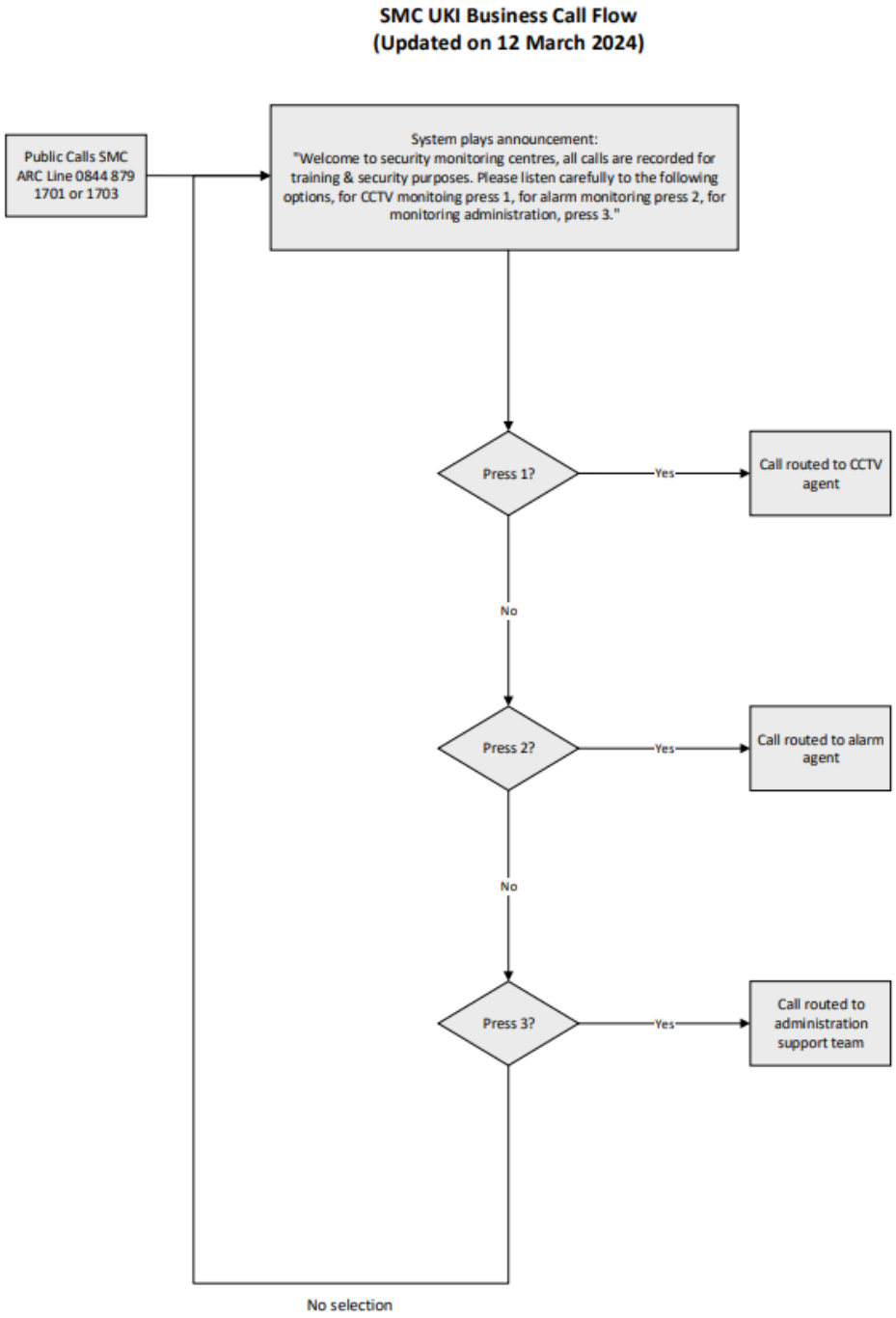
Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

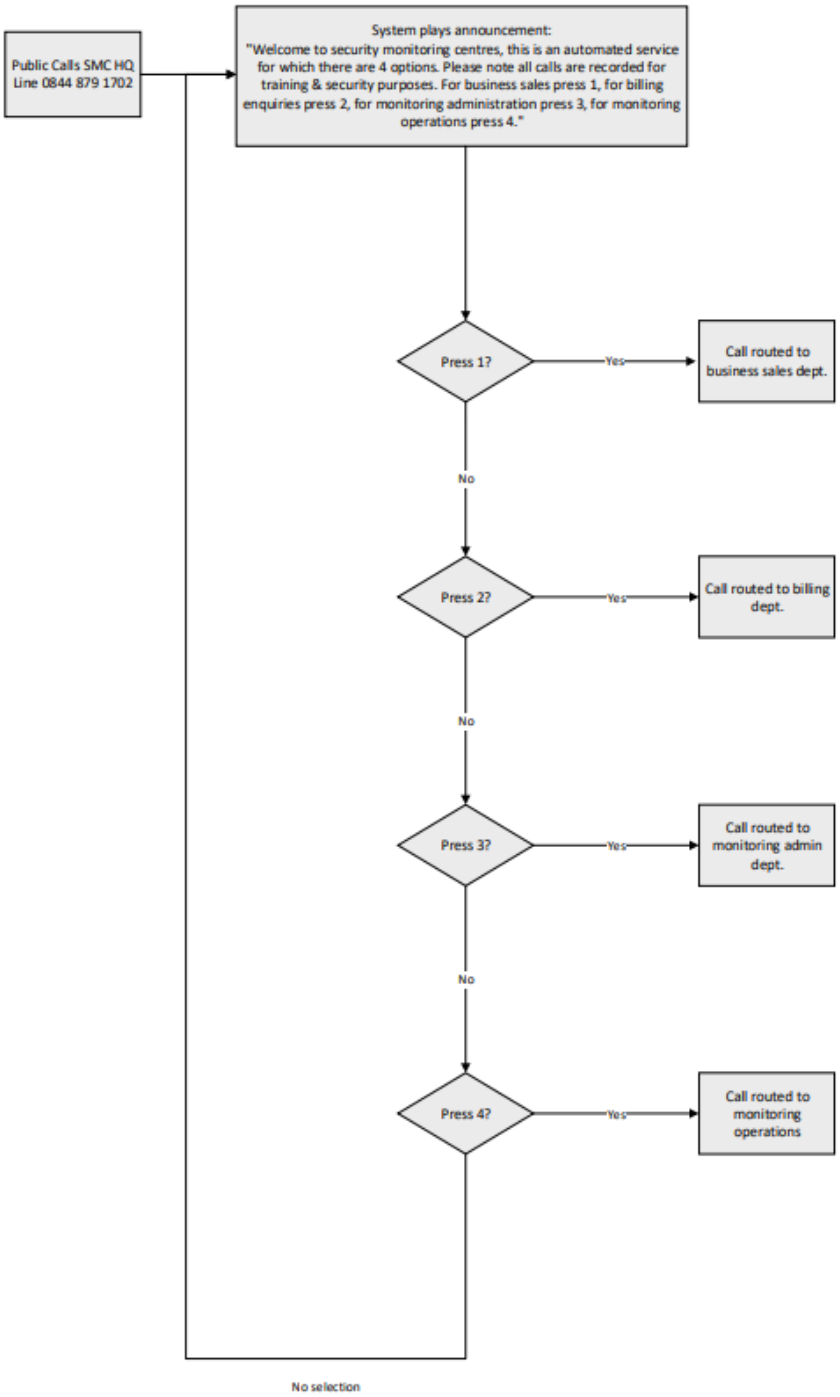
# Appendix D – Surveillance Camera Code of Practice – 12 guiding principles

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 user 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.

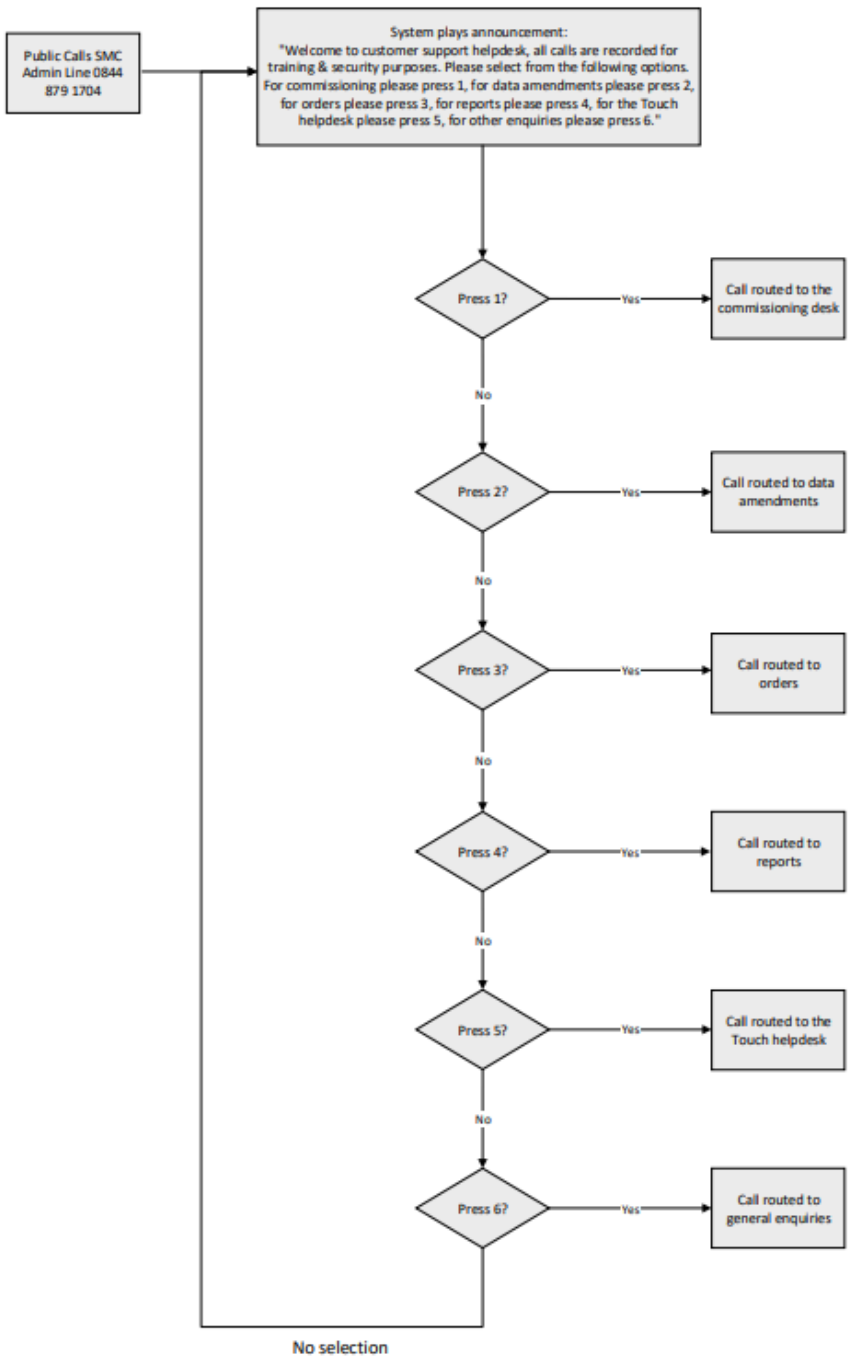
# Appendix E – SMC Telephone Call Flowcharts



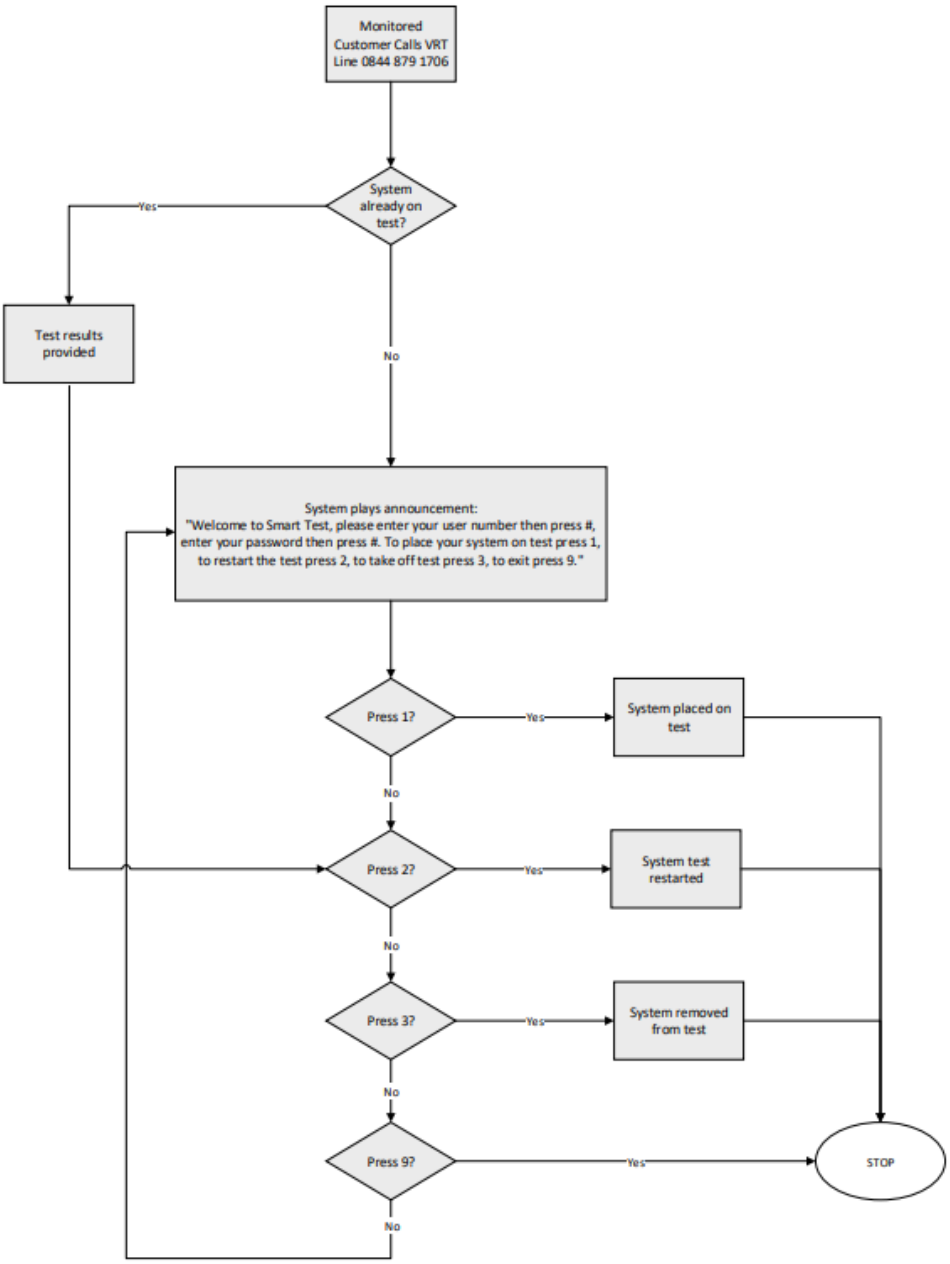
**SMC UKI Head Office Call Flow**
**(Updated on 12 March 2024)**



**SMC UKI Customer Support Call Flow**
**(Updated on 12 March 2024)**



**SMC UKI VRT Call Flow**
**(Updated on 12 March 2024)**



# Appendix F – Summary of Key changes to this document (Issue 31.0)

| | | |
|---|---|---|
| **Section 1 – SMC Monitoring** | | |
| Updated | Throughout | New SMC document template used |
| Removed | Throughout | References to the Leeds & Dublin ARC's & TSA |
| Updated | Throughout | References to BS8243:2010 updated for the 2021 version |
| Updated | Throughout | Terminology changes from SmartForm to TouchForm |
| Added | Section 1.2 | Reference to ULC standards |
| Removed | Section 1.3 | Leeds & TSA references |
| Removed | Section 1.5 | Leeds & Dublin Info |
| Added | Section 1.5 | Touch Helpdesk & SMC Vision Admin email addresses |
| Updated | Section 2.1 | DRBC schematic & text revised for new configuration |
| Removed | Section 3.2 | VRT system references |
| Updated | Section 3.4 | Caveats added for CHIP requests |
| Added | Section 3.5 | Requirements for UPG |
| Updated | Section 3.7 | Point 1 amended for current operations. |
| Updated | Section 3.9.3 | Included reference to PD6662 |
| Updated | Section 3.11.2 | Email address for Touch technical support. |
| Updated | Section 3.13 | Points 1 & 3 amended for current operations. |
| Updated | Section 3.14.3 | List of current health check reports available |
| Updated | Sections 5.3 & 5.6 | Hyperlink to CFA policy revised |
| Updated | Section 5.7 | Dates from quoted standard revised. |
| Updated | Sections 5.9.2 & 5.9.3 | BS8243 clauses revised to include 2021 edition. |
| Added | Section 5.10 Table 1 | Parameters for SP4, SP5 & SP6 devices. |
| Updated | Section 5.13 | Included HUA to 1st paragraph |
| Updated | Section 5.17 | Added SMC reservation to use log only option for persistent excessive signalling systems/sites |
| Update | Section 5.25 | BS8243 reinstatement clause revised |
| Updated | Section 6.1 | Reference to incorrect section corrected & options for on/off test updated. |
| Updated | Section 8 | Section wording amended to aid clarification |
| Updated | Section 8.3 | Updated hyperlinks |
| Updated | Section 10.3 | Updated the paragraph for TouchForms |
| Updated | Section 10.4 | Touch v2.0 Features |
| Updated | Section 10.5 | Touch v2.0 User Authority Levels & Permissions |
| Updated | Section 11.2 | Updated the paragraph for TouchForms |
| Updated | Section 11.3 | DRBC revised for new configuration |
| Removed | Section 11.4 | No longer required – TSA configuration |
| Added | Section 11.4 | ULC requirements |
| Removed | Section 12.1 | No longer required - References to TSA |
| Updated | Section 12.2.3 | Clauses 7.4.7.1 & 7.4.7.2 amended |
| Updated | Section 16 | ULC certificate added |
| **Section 2 – SMC Vision** | | |
| Removed | Section 1 | Dates on quoted standards |
| Added | Section 5.3 | CCTV schedule caveat |
| Updated | Section 15 | Sequential confirmation statement in line with 2021 edition |
| Updated | Appendix A | Privacy Notice |
| Updated | Appendix D | Surveillance Camera Code of Practice,12 guiding principles |
| Added | Appendix E | SMC Telephone Call Flowcharts |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |