Securitas Operation Centre

Operational and Administrative Manual

Table of Contents

Securitas ARC policies – important customer information

Foreword

Securitas offer a full Monitoring and Incident Management service delivered by our ARC and helpdesk teams, and we strongly recommend that our customers take advantage of the benefits a custom monitoring package brings. Where we have agreed an Incident Management service, a tailored response package will be applied, resulting in a service focused clearly on your organisation's unique requirements.

In the absence of an agreed Incident Management service, the ARC policies in this document will apply. Acceptance of Securitas Terms & Conditions indicates acceptance of all policies in this document, so you should read it carefully and agree a custom response if required.

Proper management of false alarms is vital to ensure that resource is always available to respond quickly to criminal incidents at our customer's premises, and to ensure that our entire monitored estate receives the timely responses to alarm events needed to keep your people and premises safe. It is expected that both installer and end users will co-operate with Securitas to reduce false alarms where possible, for example by staff training, ensuring that foliage is removed from detection areas, and repairing faults expediently when you are notified of them by the ARC team. Please pay careful attention to our runaway policies below, which describe the actions we will take if an alarm system sends the ARC too many false alarms for us to reasonably handle.

The standard to which the Securitas ARC is accredited (BS EN50518: Monitoring and Alarm Receiving Centres) and other related standards offer advice and guidance on ARC policy with regard to false alarm reduction. Securitas have referenced these standards and documents when formulating the following ARC policies.

It is important to note that in order to allow flexibility to respond to changes in risk and regulations, the contents of this document are subject to change without notice. If you hold a copy of this document please ensure that it is updated on a regular basis from the Securitas website.

Installers utilising the services of the Securitas ARC may use extracts from this document to inform end users of the policies and processes employed by Securitas in fulfilment of the services.

Contact Details

ARC

Telephone number 01908-658100

Email arc@securitas.uk.com

Opening times 24/7/365

ARC Admin

Telephone number 01908-658158

Email arc.admin@securitas.uk.com

Opening times 08:00 to 17:00 Monday to Friday

Technical Helpdesk

Telephone number 08081686486

Email Technical.Servicedesk@securitas.uk.com

Opening times 24/7/365

Standard ARC responses

Customers with unique alarm response requirements are welcomed by Securitas, and these requirements will be assessed and agreed by your Account Manager in conjunction with the ARC Management team. In the absence of agreed custom response requirements, the Securitas ARC will carry out the following actions in response to specified alarm types:

Description	Action
Fire Alarm (intruder alarm status known, site open)	Site for 60s, Fire Service (if required or no answer from site)
Fire Alarm (intruder alarm status known, site closed)	Fire Service, Keyholder
Fire Alarm (intruder alarm status unknown, inside normal business hours*)	Site for 60s, Fire Service (if required or no answer from site)
Fire Alarm (intruder alarm status unknown, outside of normal business hours*)	Fire Service, Keyholder
Hold Up or confirmed holdup (Personal Attack)	Police (URN required), Keyholders
Hold Up (Panic Attack) – system requiring intervention	As per Police / Installer requirements N.B. telephone call back as a single method of confirmation Is no longer acceptable to Police Services for reinstatement of systems installed in commercial premises.
Unconfirmed Intruder	Keyholder (120s filter) except Southern Ireland (60s filter)
Confirmed Intruder (with URN)	Police, Keyholder (120s filter) except Southern Ireland (60s filter)
Confirmed Intruder (no or suspended URN)	Keyholder (120s filter) except Southern Ireland (60s filter)
Tamper (site open)	Site (to advise contact installer), Remote Diagnostics and repair (if available), Installer via email
Tamper (site closed)	Keyholder, Remote Diagnostics and repair (if available), Installer via email (if required),
Mains Power Fail (site open)	Site, Keyholder if required
Mains Power Fail (site closed)	Keyholder
Low Battery (site open)	Site, Keyholder (if required), Installer (via email)
Low Battery (site closed)	Keyholder, Installer (via email)
Comms Fail (site open) – dual path system	Site, Installer if required
Comms Fail (site closed) – dual path system	Keyholder if required, Site (09:00 next working day for single path fail on dual path system)
Comms Fail (site open) – single path system	Site, installer if required
Comms Fail (site closed) – single path system	Keyholder, installer if required
Comms Fail followed by Unconfirmed Intruder	Police (URN and Dual path system required), Keyholder
Unconfirmed Intruder followed by Comms Fail	Police (URN required), Keyholder
Zone Omit (site closed)	Keyholder

Zone Omit (site open)	Log only
System Fault (site open)	Site (to advise contact Installer), Remote Diagnostic and repair (if available), Installer by email
System Fault (site closed)	Remote Diagnostic and repair (if available), Keyholder, Installer by email
24hr alarm zone (door contact, site open)	Log only
CCTV	Review activation, then: **Crime in progress** – Police, Keyholder **Nothing seen** - No further action **Persons seen (open site)** – audio warn-off, monitor 60s, then NFA or keyholder dependant on activity **Persons seen (physically secured site)** – audio warn-off, keyholder
CCTV System Fault	Installer
Late to Close Alert	Keyholder
Late to Test	Installer (via email)

* Normal business hours – 08:00 – 18:00 Mon-Fri

<u>Supported products</u>

The Securitas ARC has the ability to monitor all standard intruder alarm transmitters provided by UK Alarm Transmission Providers, and the vast majority of CCTV devices as defined by the Sureview Systems integrated products list for Immix https://sureviewsystems.com/partners/. We can also manage the majority of intercom types used in the UK market. All devices integrated to our ARC systems have been extensively tested for compatibility and reliability. Should you wish to connect a device for monitoring or response which is not presently supported, please contact our ARC Admin team for assistance. We are not liable for any failures or losses due to the connection of unsupported devices.

<u>Intruder alarm filtering policy</u>

In line with UK industry standards, it is the policy of the Securitas ARC to filter all intruder alarm signals (both confirmed and unconfirmed) for 120 seconds (60 seconds for systems in Southern Ireland). During this filtering period, no action will be taken to handle the alarm and the alarm will not normally be visible to the ARC Controllers.

On receipt of an Open signal from the system, all filtered alarms from that site will be cancelled and will remain logged in account history, with no action being taken to handle the alarm.

Should the filtering period pass without an Open signal having been received, the alarm/s will then immediately be presented to a Controller for action.

Although filtering of intruder alarm activations is a standard practice across the ARC industry, you are strongly recommended to advise your insurance company of the Securitas ARC filtering policy.

Fire intervention Policy

Many Fire Services now require us to contact the monitored premises when we receive a fire alarm signal to confirm that the cause of the alarm is a genuine fire, especially during normal working hours where the site being monitored is a commercial premises.

If we are unable to confirm a fire in this way, many Fire Services will refuse to attend at our request unless they receive an additional confirmation from the premises that their attendance is required. For this reason, we ask that you advise all building occupants that if the fire alarm activates and Fire Service attendance is required, they must call 999 to request Fire Services even if their alarm is monitored.

Communications fail filtering policy

A single communications path failure signal (with no other associated signals or alarms) will be cancelled and no action taken by the Securitas ARC if a restore is received for the failure within the following timescales:

Redcare Classic/GSM	60 seconds
I.P. over corporate LAN	60 seconds
I.P. over ADSL	300 seconds
Generic radio (GPRS/GSM) dual path system	1200 seconds
Generic radio (GPRS/GSM) single path system	60 seconds

Keyholder contact policy

Securitas normally require our customers to provide a minimum of 2 and a maximum of 5 keyholders per monitored account (unless keyholding response is provided by a keyholding service with a 24/7 control room, in which case a single keyholder will be acceptable). These keyholders may be customer staff or a keyholding company, or a mixture of both.

Police requirement for premises protected by Intruder alarm which has been issued with a Police Unique Reference Number (URN) is that a minimum of 2 keyholders should be capable of attending the premises within 20 minutes of receiving a request to attend from the Securitas ARC.

The Securitas ARC uses an IVR system to deal with keyholder notification of alarm events. The IVR system will call the contact/keyholders and notify them of the full address of the site and the alarms which have been received. The recipient of the IVR call must then press 8 on their telephone keypad to accept the call. In the event that the recipient does not answer or does not press 8 the system will call the next contact/keyholder on the list. In the event all contacts/keyholders have been called and none of them accept the alarm, the system will sleep the alarm and try again after 5 minutes. In this way, attempts will be made by the system to contact each keyholder up to three times. If no keyholder accepts the call the alarm will be passed to an operator, who will attempt to contact each keyholder once, for a maximum of 60 seconds, leaving a message if the call is not accepted. At this stage, the alarm will be deemed to have been handled, and will be cleared on the system with the disposition “Unable to contact keyholder”. A report will be provided to all customers daily on any alarms which have been closed with this disposition code.

Once contact has been made with a keyholder, responsibility for carrying out any required action (e.g. visiting the premises to investigate the alarm condition or reset the alarm) will rest with that keyholder.

Although Securitas will make every attempt to ensure that records are accurate, it is the responsibility of our customers to ensure that the Securitas ARC has up to date information regarding keyholder names and contact details. Listed keyholders must be easily contactable and available to attend upon request. The ARC must be informed in advance when a keyholder is temporarily unavailable (e.g. on annual leave).

When attempting to contact a keyholder, the ARC will call keyholders and use contact numbers in the order listed in the alarm handling system. Please ensure when communicating contact numbers, the numbers are listed in the preferred order.

Keyholder verification

Securitas strongly recommend using a password based system to secure telephone communication between ARC operators and keyholders or system end users. In the event that a keyholder or end user does not have or is unwilling to share their password with our ARC operators, we will attempt to verify their credentials by requesting and receiving a minimum of two out of the three following:

- System Account number
- Name of another keyholder on the account
- Postcode of the protected premises

If the keyholder is unable or unwilling to pass on this information, the call will be terminated and no information passed. Please note that it will hamper our ability to successfully protect your people and premises if keyholders are unwilling to give us verification details. Keyholders must be made aware in advance that we may call them 24/7 and request such details. Securitas will not accept liability for any losses howsoever caused if keyholders refuse to provide suitable verification information.

CCTV monitoring policy

Unwanted CCTV alarm activations are the main source of delay to alarm response. To this end, unless otherwise negotiated prior to contract start, CCTV systems monitored by the Securitas ARC should comply with the following requirements:

- Protected area is physically secured so that expected or authorised activity cannot activate the triggering device/s
- Staff/site users have the ability to unset the system before entering the protected area pursuant to 1) above (there should be a visual indication to staff from which they can ascertain whether or not the system is armed)
- Customer and end user accepts ARC runaway alarm policies (see below)
- Customer and end user agrees to respond within 3 working days to ARC requests to rectify issues causing false alarm activations (e.g. cut back foliage etc).

Exceptions to the conditions above must be agreed on an individual basis and may lead to additional cost for the service.

CCTV acceptance policy

CCTV systems which are newly installed (whether by Securitas or third party installers) will be subject to a soak test period, during which the performance of the system will be assessed and any issues with system performance will be addressed. During the soak test, system performance including alarm volumes will be assessed and the CCTV system may be accessed by the ARC team, but the ARC will not respond to any alarm activations (unless criminal activity can be seen at the time the system is accessed).

The soak test process is as follows:

- Initial performance assessment made over the first 7 day period of operation. If system performance is satisfactory and false alarm volumes within acceptable limits, the system will be accepted into service and live monitoring with the agreed response will commence
- If any performance issues are noted during the first 7 days of operation, the system will not be accepted into service, and the root cause of the issues will be rectified by the customer or their nominated installer. Once the customer or their nominated installer has notified us that all issues have been resolved and soak testing can be re-commenced, performance will be reviewed again over the following 7 day period.

Any further issues which have not been addressed within the extended 14 day soak test will be discussed and required actions agreed with the customer or their nominated installer before the system is accepted into service.

CCTV systems which are already operational when taken over from another ARC will be monitored immediately without a soak test, provided that system performance can be assessed prior to takeover using information from the losing ARC. System performance will in this case be monitored whilst the system is live, and any performance issues which were unknown prior to takeover will be raised by the ARC and must be addressed within the first 14 days of operation. Where required, the CCTV runaway policy will be applied during this period (see below).

CCTV systems will be checked for efficacy at least monthly on a best-endeavours basis, and installers notified of any errors found.

CCTV runaway policy

The Securitas ARC operates the following policy with regard to CCTV activations caused by authorised or expected activity:

If a single camera detector causes multiple activations to be received in any 30 minute period where that activation is not caused by unauthorised or unexpected activity, Securitas reserves the right at our discretion to disable that camera (or detector) for a period of time appropriate to the issue. This will always be a last resort, but in the event that this becomes necessary, we will notify you of the action taken by email to a pre-agreed email address. You may be required to take some action (e.g. to cut back foliage) before we will re-activate the detector, and if this is needed we will tell you what has to be done when we inform you that the detector has been disabled. It is your responsibility to inform us that the action has been taken so we can re-activate the detector.

In the event that the reason for the false alarms cannot be determined remotely, the detector or camera will be disabled according to the following escalating schedule, assuming that the issue re-occurs with 24 hours after camera / detector re-enablement:

- 2 hours
- 4 hours
- 8 hours
- Until we are notified by the customer that the issue has been resolved

Securitas will not be liable for any losses howsoever caused during periods in which cameras or detectors are disabled if the failure to detect an event was caused by the required disabling or a camera or detector pursuant to our CCTV runaway policy.

Audio warn-off policy

We may use audio warn-off (if fitted) to inform a potential trespasser that they should leave the premises. We will normally do this by exception only, and only if it is clear to the subject of the warn-off that they are trespassing (i.e. the area is physically protected by fencing).

If we see criminal activity, we will not normally send an audio warn-off, as our preference should a crime be committed is to contact the Police and have the person or people committing the crime arrested.

Intruder alarm runaway policy

Securitas reserve the right at our discretion to disable monitoring of an alarm zone or system if we are receiving multiple activations from that zone or system, howsoever caused. If we take this action we will inform you of the action taken either by telephone or by email to a pre-agreed email address. Generally, if a zone is disabled, it will automatically be re-enabled when the alarm is re-set, but if a whole system is placed on test, you may have to take some action to fix the problem before we re-enable monitoring. If you do need to take some action, we will take you what this action is, and you will need to tell us that this has been done before we re-enable monitoring.

New connections

All new connections must be processed using our standard new connection forms and emailed to arc.admin@securitas.uk.com. We aim to process all new connection forms the same working day if received by 3pm, or the next working day otherwise. Depending on the connection type and manufacturer, it will take up to 10 working days for the transmitter to be delivered, and these timescales are outside of our control.

Volume transfers

New connections of larger estates comprising 10 or more systems can be notified to us using a spreadsheet or database transfer. Please contact our admin department at arc.admin@securitas.uk.com to agree this prior to sending, and please note that timescales for processing volume transfers can be considerably longer than single site connections. Timescales will be agreed prior to commencement of the process.

As a minimum, volume transfer data must include:

- Site name and address
- Site contact details
- Keyholder contact details (min 2, max 5)
- Transmitter type and ID number
- Police / Fire Service
- URN numbers and status (if required)
- Remote reset status (if required)
- Zone programming details
- Site open / close times (commercial premises)
- Panel type and IP address (for remote connection and control)
- IP address details (CCTV)
- Ports used including protocol and direction (CCTV)
- Username and password (CCTV)
- Site code (CCTV, Adpro only)
- Intercom programming and line numbers (if required)

You will also need to ensure that the incumbent ARC has been notified of the impending transfer, and that permission has been given for the incumbent to discuss the detail with our admin team.

Engineer verification

Engineers contacting the Securitas ARC (e.g. to place systems on test or commission new systems) are validated by the industry standard method of engineer name and pin number / password. It is the responsibility of all installers to supply us with accurate and up to date engineer lists to facilitate engineer verification. Engineer who do not present the correct name and pin number / password will be directed to obtain these details and call back before any changes are made to the system or status (i.e. on test etc.).

Engineering tests

Security systems (including fire monitoring systems) are tested from time to time. Securitas Systems Engineers are well versed in the requirements of the ARC, but if you employ a third party maintenance company to install and maintain your system, or if your own staff are used to carry out testing (e.g. weekly fire or Panic Alarm tests) then they must abide by the following conditions:

The Securitas ARC must be notified prior to any testing being carried out, in order that we place the system "On Test" and do not respond to an alarm test as if it were notification of a genuine alarm. The ARC may be notified by one or more of the following methods:

- By telephone
- By use of MASweb

During the chosen testing period, and until you (or your appointed agent) notify the ARC that the test has been completed, the system which is the subject of the test will not be monitored, and the ARC will not respond to any activations which are generated by the system. If a genuine incident occurs during the testing period (e.g. a fire at the premises whilst the fire alarm is on test), you must call the emergency services or other response agency as appropriate.

After testing is completed, you (or your appointed agent) must notify the ARC that the test is complete in order that monitoring is resumed. The default test period is normally 1 hour, after which the ARC systems will normally automatically resume monitoring. For this reason, you or your agent must notify the ARC if the test period exceeds either 1 hour or the time originally agreed for the test, whichever period is the shorter.

We may require you to use MASweb or to place systems on test if you regularly carry out testing. You will be responsible for any activity required to ensure that this web based system is accessible from your premises.

Call recording policy

All telephone calls to and from the Securitas ARC are recorded as per the requirements of EN50518, for quality assurance, training and investigation purposes. Such recordings are for internal use only and it is not Securitas policy to release call recordings externally to customers or other agencies, unless required to do so by law.

Customers are requested to inform all staff who may have contact with the Securitas ARC of the ARC call recording policy.

Remote alarm panel connections

Securitas will always seek where possible to provide a remote connection to intruder and CCTV systems, in order to facilitate remote maintenance and fault resolution (where Securitas are the maintainer). Remote diagnostics and maintenance facilities are also available for installers (please contact ARC admin for details**). Remote connections give the ARC the ability to control various functions of the system (dependant on device type), but use of these functions e.g. arming, zone isolation etc. will not normally form part of the ARC service, unless agreed as part of a tailored Incident Management service.

Access control

The Securitas ARC may have the ability to remotely open doors or gates for your staff or approved agents, either to a fixed schedule or manually when required. Special equipment is needed to allow us to do this, so this must be agreed and costed at survey if it is required.

Where this service is utilised, it is very important that a password system is used so we can be sure that the person requiring access is entitled to be on the premises. You must ensure that these passwords are correctly managed (e.g. changed when a staff member leaves the business) and that the ARC is notified in writing when the password changes.

Securitas will not be liable for any losses, whether direct or indirect, due to us allowing a person access to a premises, unless we are careless or fail to exercise an appropriate level of skill in carrying out this service.

Any liability in any case will be subject to the limits stated in the terms and conditions of your Securitas contract.

Remote Resets

Securitas ARC operators have the ability in some cases to remotely reset alarm systems, either by direct access to the panel utilising the UDL capability of the alarm transmission equipment, or by provision of an anticode which is to be keyed into the panel by an end user.

On receipt of a telephone request for a remote reset by an end user, our ARC operators must ensure that we comply with the requirements of BS 8473:2006+A1:2008 in providing this service. This means that we can only provide the facility for a remote reset following a confirmed intruder alarm on a maximum of two occasions during a rolling 12 month period. Remote resets following activation of an unconfirmed intruder alarm are not subject to these limits, but may be subject to fair usage and intruder alarm runaway limits.

Callers requesting a Remote Reset must provide verification information before a remote reset is authorized. If we are unable to verify the identity of the requestor, no remote reset will be provided and the caller will be asked to contact their installer for assistance. Verification will be confirmed by provision of the following:

- The Account Number
- The Account or Keyholder code word
- The Account Name and Address
- The Engineer's ID Number (if appropriate)

The caller will then be asked the reason for the activation, and this response will be recorded in the account history.

If a remote reset cannot be provided or is for any reason unsuccessful, the requestor will be required to contact their installer for assistance.

Out of hours installer service desk

Our SOC is able to offer an additional service to installers for the handling of out of hours service requests from their clients.

Unless a custom process is defined for this service, our standard actions are as follows:

On receipt of a call from your customer, we will take their name, address, contact name and number, reference numbers and what their issue is. These details will be entered onto our system, whereby a message will be raised. We shall contact the on call engineer via telephone. If we are unable to contact the engineer we will continue to call them every 15 minutes. After 3 attempts we will proceed to call the company's escalation contacts.

Use of this facility is subject to additional costs – please contact ARC admin for details.

Lone worker monitoring services

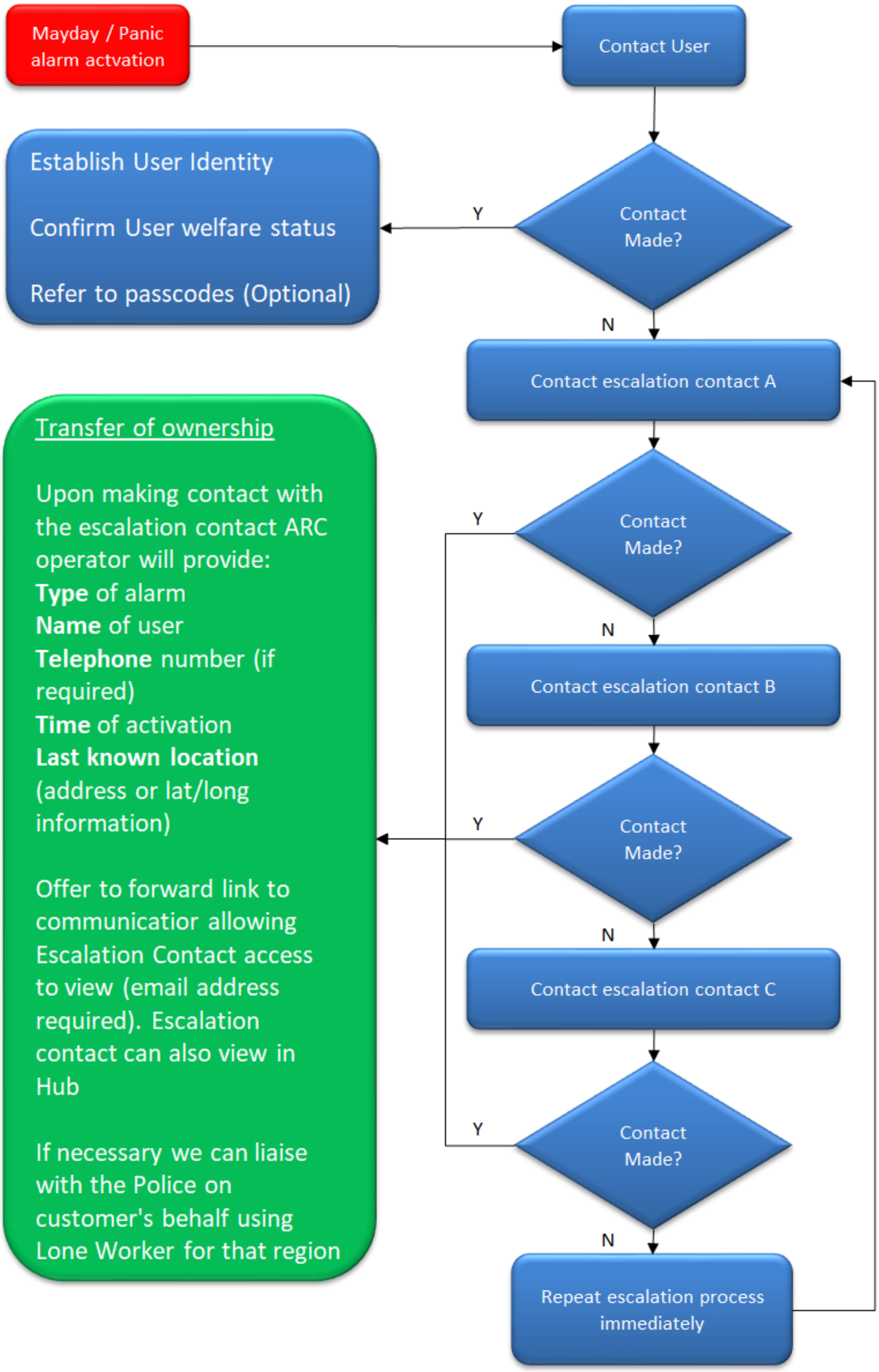
We can supply a range of Lone Worker Devices and smartphone applications to offer protection at all risk levels.

Securitas manage and verify alarms on a daily basis for customers and complies with the BS8484:2016 – Provisions for Monitoring Lone Workers standard. Securitas offer a tailored escalation plan for each and every customer according to their individual and unique needs and will assess a response plan against the identified risks.

Our dedicated team at the Securitas Operations Centre have experience in deploying thousands of Lone Worker Solutions.

When a customer requires a lone worker solution, we complete an optional unique risk assessment and evaluate People, Environment and Tasks (the PET model) to ensure that we provide the most suitable product for our customers' level of risk.

We create an escalation response plan for lone workers, which are unique to our clients; and tailored to your individual requirements. Our default escalation procedure for an emergency alarm which can apply to both on site and traveling staff members is shown on the next page.



Mayday / Panic alarm actvation

Contact User

Contact Made?

Establish User Identity

Confirm User welfare status

Refer to passcodes (Optional)

Contact escalation contact A

Contact Made?

Contact escalation contact B

Contact Made?

Contact escalation contact C

Contact Made?

Repeat escalation process immediately

Transfer of ownership

Upon making contact with the escalation contact ARC operator will provide:
Type of alarm
Name of user
Telephone number (if required)
Time of activation
Last known location (address or lat/long information)

Offer to forward link to communicatior allowing Escalation Contact access to view (email address required). Escalation contact can also view in Hub

If necessary we can liaise with the Police on customer's behalf using Lone Worker for that region

General Data Protection Regulation

Securitas are committed to ensuring the privacy and safety of personal data in compliance with the applicable data protection legislation. Please click on the link below to review our Privacy Policy:

https://www.securitas.uk.com/News/lead/privacy-policy/

Please note that client records stored in our ARC accounts are held for the duration of the contract plus two years, in accordance with BS8591.

Liability

Your security system is designed to reduce the risks of loss or damage to your premises so far as this can be done by the use of this type of equipment. However we do not guarantee that the system cannot be removed, tampered with or made to stop working by you or by any unauthorised person. If this happens, we are not responsible for any losses you may suffer directly or indirectly.

We do not guarantee to you that:

(a) particular losses or injuries will be prevented by using the system; or

(b) that the system will work continuously and without error, in particular where interruptions or errors are due to something beyond our reasonable control.

The products we use are designed and manufactured to high standards. However, even these products, like all mechanical and electronic devices, can develop faults, and as such we cannot guarantee a fault-free service.

We do not know the value of your premises or its contents and the purpose of installing your security system is not to act as insurer of your premises or your contents, or contents held at your premises by third parties.

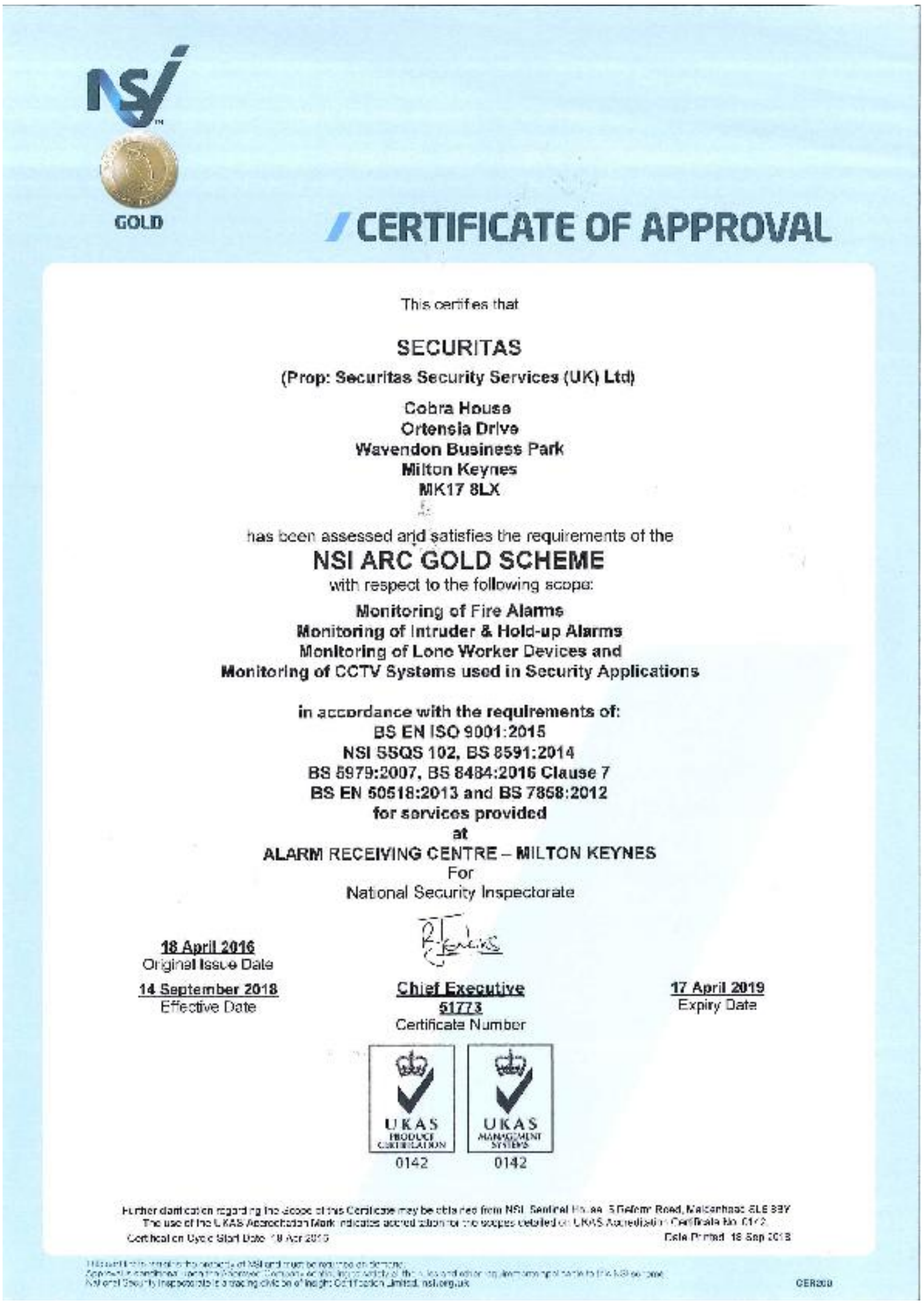
We accept that we must make sure that the system is of satisfactory quality, that it is suitable for the purpose and that the system will meet with the description provided before it was installed.

ARC accreditations

The Securitas ARC is accredited to the following standards:

BS EN50518-1:2013 Pts 1-3	Monitoring and Alarm Receiving Centres
BS8591:2014	Remote Centres receiving signals from alarm systems
BS8484: 2016	Provision of Lone Worker Services
Certics (PSA)	
ISO 27001:2013	Information Security Management
IS0 14001:2015	Environmental Management
OHSAS 18001:2007	Occupational Health and Safety management systems
SIA Approved Contractor	

Please see below for certification details



GOLD

CERTIFICATE OF APPROVAL

This certifies that

SECURITAS
(Prop: Securitas Security Services (UK) Ltd)

Cobra House
Ortensia Drive
Wavendon Business Park
Milton Keynes
MK17 8LX

has been assessed and satisfies the requirements of the

NSI ARC GOLD SCHEME

with respect to the following scope:

Monitoring of Fire Alarms
Monitoring of Intruder & Hold-up Alarms
Monitoring of Lone Worker Devices and
Monitoring of CCTV Systems used in Security Applications

in accordance with the requirements of:
BS EN ISO 9001:2015
NSI SSQS 102, BS 8591:2014
BS 5979:2007, BS 8484:2016 Clause 7
BS EN 50518:2013 and BS 7858:2012
for services provided
at
ALARM RECEIVING CENTRE – MILTON KEYNES

For
National Security Inspectorate

18 April 2016
Original Issue Date

14 September 2018
Effective Date

Chief Executive

51773
Certificate Number

17 April 2019
Expiry Date

UKAS PRODUCT CERTIFICATION
0142

UKAS MANAGEMENT SYSTEMS
0142

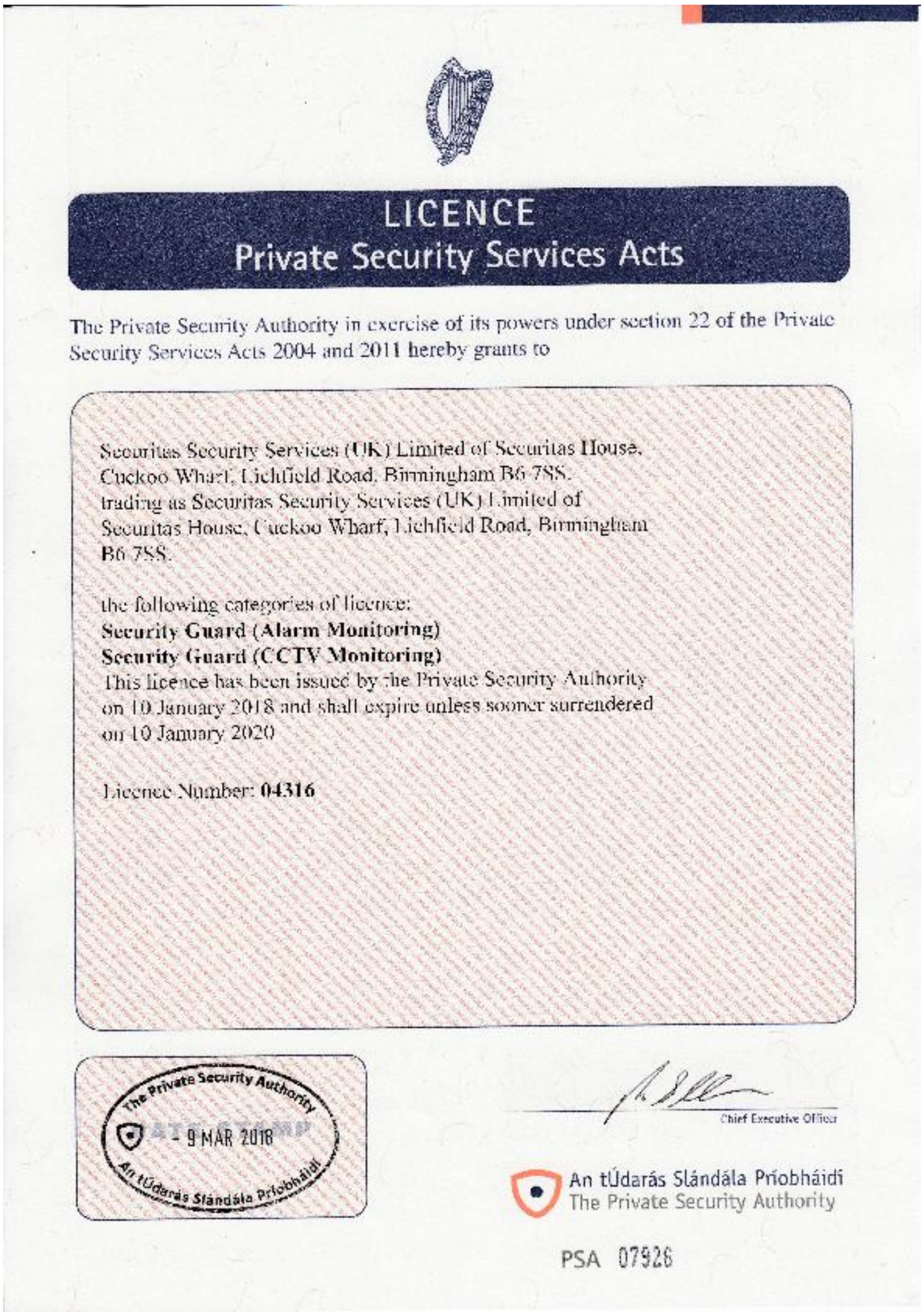
Further clarification regarding the scope of this Certificate may be obtained from NSI, Sentinel House, 5 Reform Road, Maidenhead SL6 8BY
The use of the UKAS Accreditation Mark indicates accreditation for the scopes detailed on UKAS Accreditation Certificate No. 0142.

Certification Cycle Start Date 18 Apr 2016

Date Printed 18 Sep 2018

This certificate remains the property of NSI and must be returned on demand.
Approval is conditional upon the Approved Company complying strictly with the rules and other requirements applicable to the NSI scheme.
National Security Inspectorate is a trading division of Insight Certification Limited. nsi.org.uk

CER200



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

Securitas Security Services (UK) Limited of Securitas House, Cuckoo Wharf, Lichfield Road, Birmingham B6 7SS.
trading as Securitas Security Services (UK) Limited of Securitas House, Cuckoo Wharf, Lichfield Road, Birmingham B6 7SS.

the following categories of licence:
Security Guard (Alarm Monitoring)
Security Guard (CCTV Monitoring)
This licence has been issued by the Private Security Authority on 10 January 2018 and shall expire unless sooner surrendered on 10 January 2020

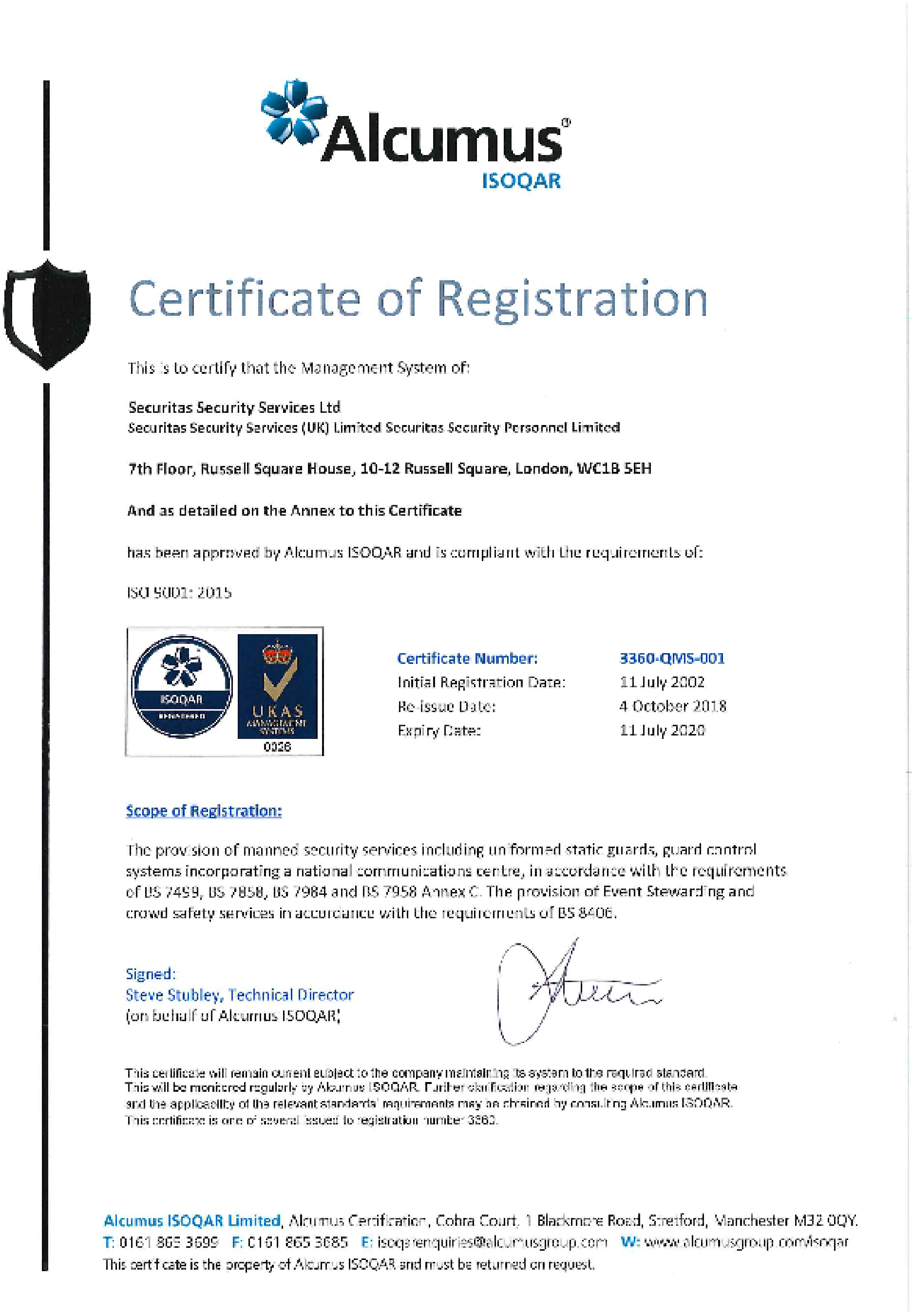
Licence Number: **04316**

The Private Security Authority
DATE STAMP
- 9 MAR 2018
An tÚdarás Slándála Príobháidí

Chief Executive Officer

An tÚdarás Slándála Príobháidí
The Private Security Authority

PSA 07926



Alcumus
ISOQAR

Certificate of Registration

This is to certify that the Management System of:

Securitas Security Services Ltd
Securitas Security Services (UK) Limited Securitas Security Personnel Limited

7th Floor, Russell Square House, 10-12 Russell Square, London, WC1B 5EH

And as detailed on the Annex to this Certificate

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

ISO 9001: 2015

Certificate Number:	**3360-QMS-001**
Initial Registration Date:	11 July 2002
Re-issue Date:	4 October 2018
Expiry Date:	11 July 2020

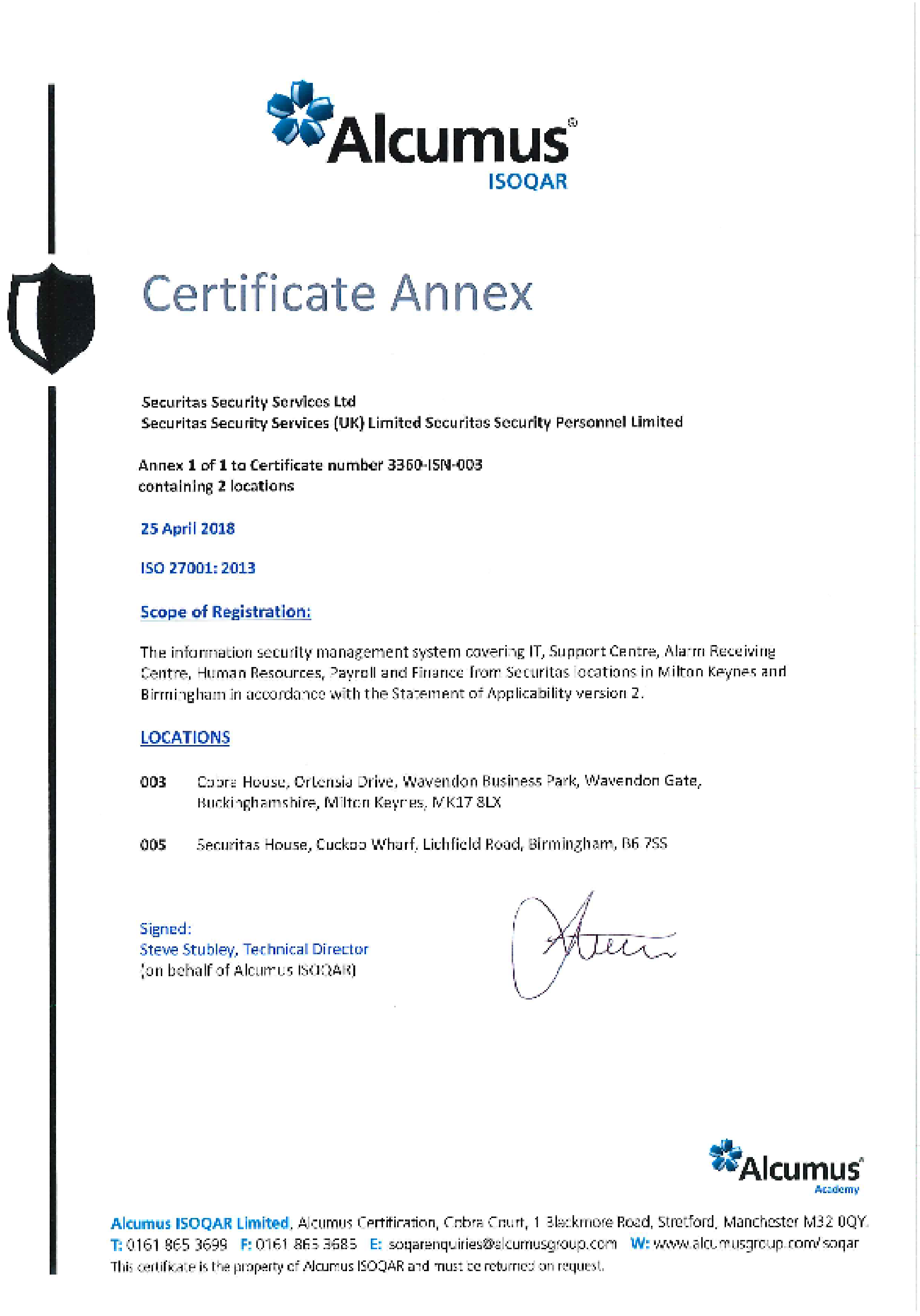
Scope of Registration:

The provision of manned security services including uniformed static guards, guard control systems incorporating a national communications centre, in accordance with the requirements of BS 7499, BS 7858, BS 7984 and BS 7958 Annex C. The provision of Event Stewarding and crowd safety services in accordance with the requirements of BS 8406.

Signed:
Steve Stubley, Technical Director
(on behalf of Alcumus ISOQAR)

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting Alcumus ISOQAR. This certificate is one of several issued to registration number 3360.

Alcumus ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com W: www.alcumusgroup.com/isoqar
This certificate is the property of Alcumus ISOQAR and must be returned on request.



Alcumus ISOQAR

Certificate Annex

Securitas Security Services Ltd
Securitas Security Services (UK) Limited Securitas Security Personnel Limited

Annex 1 of 1 to Certificate number 3360-ISN-003
containing 2 locations

25 April 2018

ISO 27001: 2013

Scope of Registration:

The information security management system covering IT, Support Centre, Alarm Receiving Centre, Human Resources, Payroll and Finance from Securitas locations in Milton Keynes and Birmingham in accordance with the Statement of Applicability version 2.

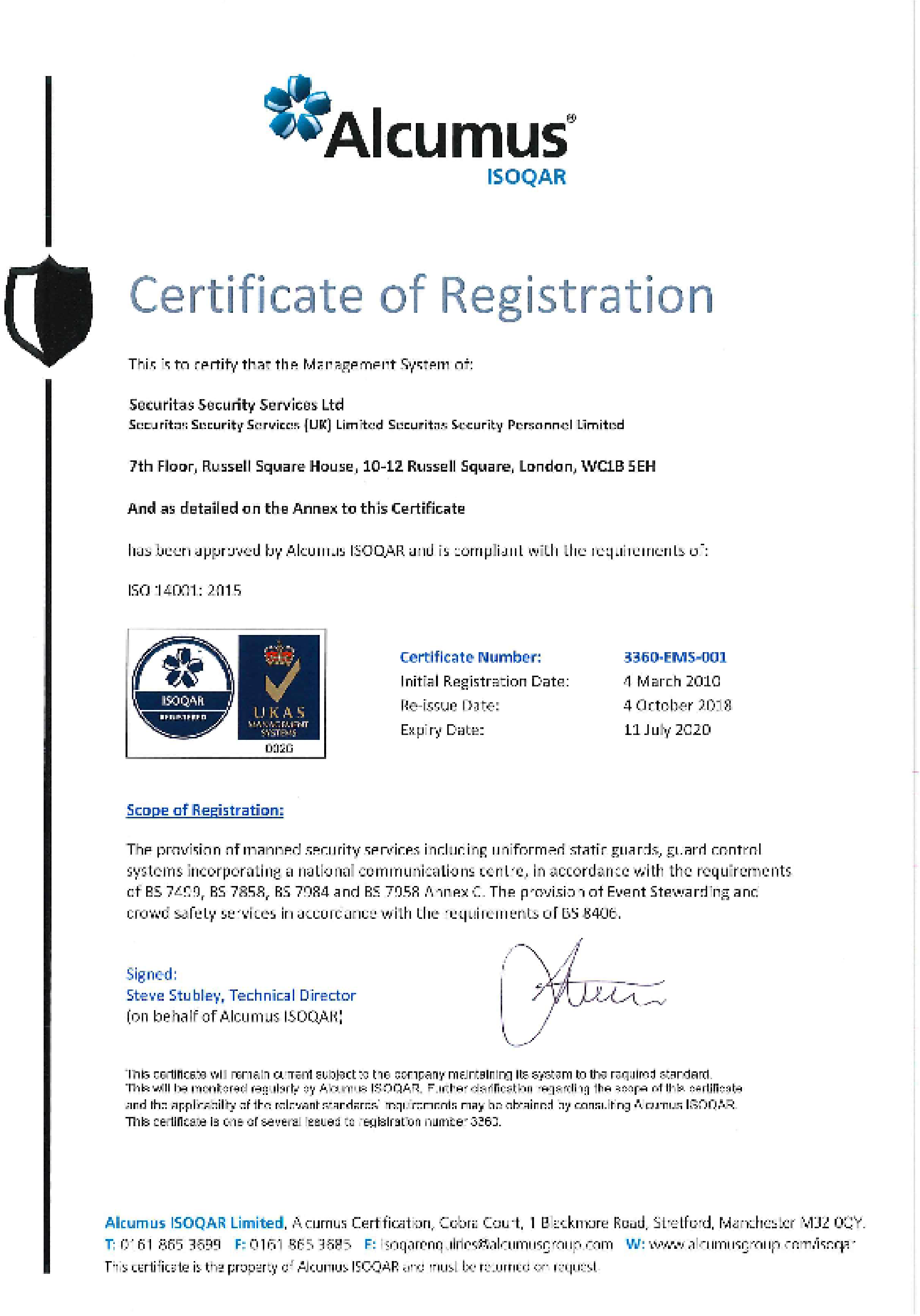
LOCATIONS

003	Cobra House, Ortensia Drive, Wavendon Business Park, Wavendon Gate, Buckinghamshire, Milton Keynes, MK17 8LX
005	Securitas House, Cuckoo Wharf, Lichfield Road, Birmingham, B6 7SS

Signed:
Steve Stubley, Technical Director
(on behalf of Alcumus ISOQAR)

Alcumus Academy

Alcumus ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: soqarenquiries@alcumusgroup.com W: www.alcumusgroup.com/soqar
This certificate is the property of Alcumus ISOQAR and must be returned on request.



Alcumus
ISOQAR

Certificate of Registration

This is to certify that the Management System of:

Securitas Security Services Ltd
Securitas Security Services (UK) Limited Securitas Security Personnel Limited

7th Floor, Russell Square House, 10-12 Russell Square, London, WC1B 5EH

And as detailed on the Annex to this Certificate

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

ISO 14001: 2015

Certificate Number:	**3360-EMS-001**
Initial Registration Date:	4 March 2010
Re-issue Date:	4 October 2018
Expiry Date:	11 July 2020

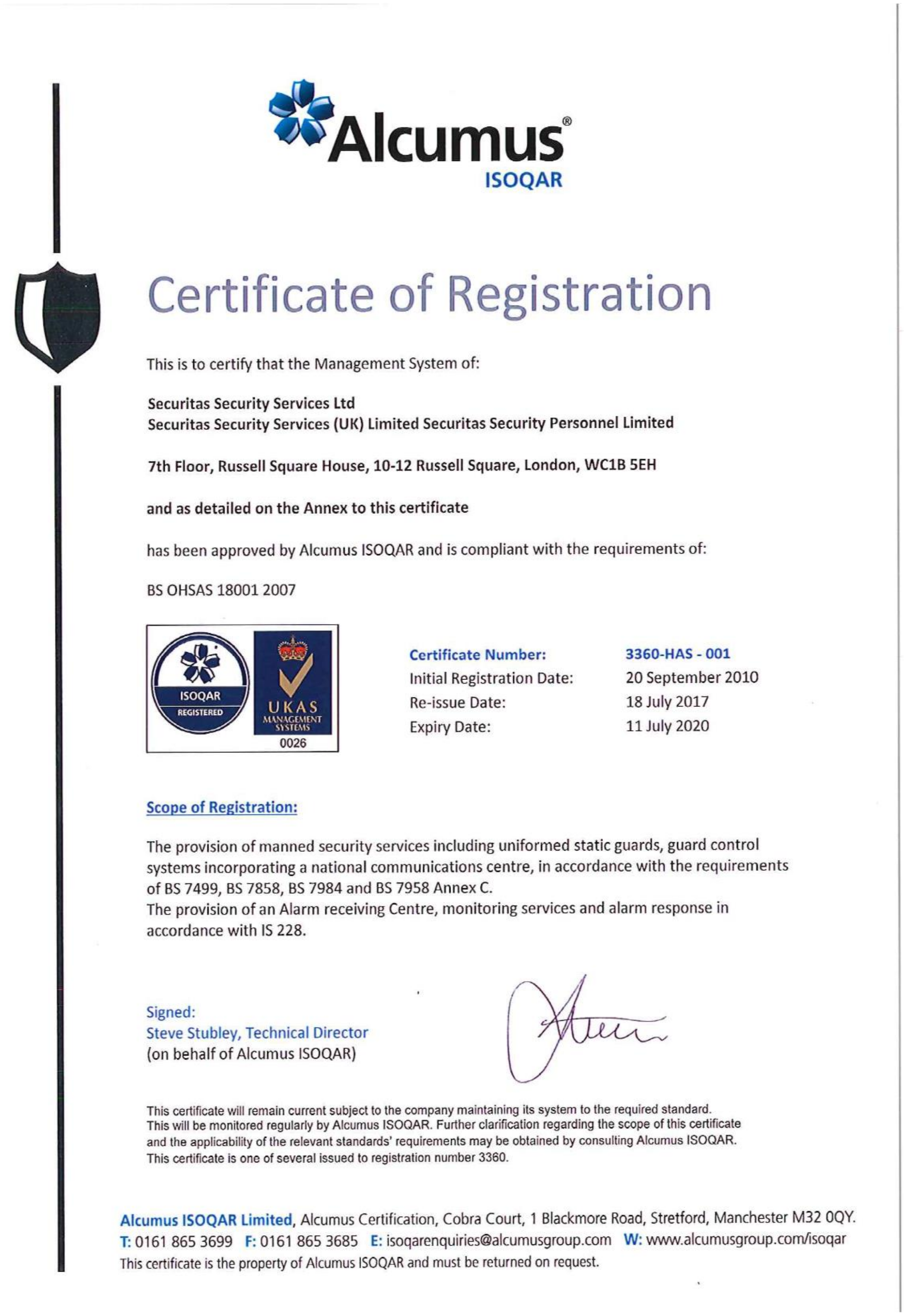
Scope of Registration:

The provision of manned security services including uniformed static guards, guard control systems incorporating a national communications centre, in accordance with the requirements of BS 7499, BS 7858, BS 7984 and BS 7958 Annex C. The provision of Event Stewarding and crowd safety services in accordance with the requirements of BS 8406.

Signed:
Steve Stubley, Technical Director
(on behalf of Alcumus ISOQAR)

This certificate will remain current subject to the company maintaining its system to the required standard.
This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting Alcumus ISOQAR.
This certificate is one of several issued to registration number 3360.

Alcumus ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com W: www.alcumusgroup.com/isoqar
This certificate is the property of Alcumus ISOQAR and must be returned on request.



Alcumus ISOQAR

Certificate of Registration

This is to certify that the Management System of:

Securitas Security Services Ltd
Securitas Security Services (UK) Limited Securitas Security Personnel Limited

7th Floor, Russell Square House, 10-12 Russell Square, London, WC1B 5EH

and as detailed on the Annex to this certificate

has been approved by Alcumus ISOQAR and is compliant with the requirements of:

BS OHSAS 18001 2007

ISOQAR REGISTERED · UKAS MANAGEMENT SYSTEMS 0026

Certificate Number:	**3360-HAS - 001**
Initial Registration Date:	20 September 2010
Re-issue Date:	18 July 2017
Expiry Date:	11 July 2020

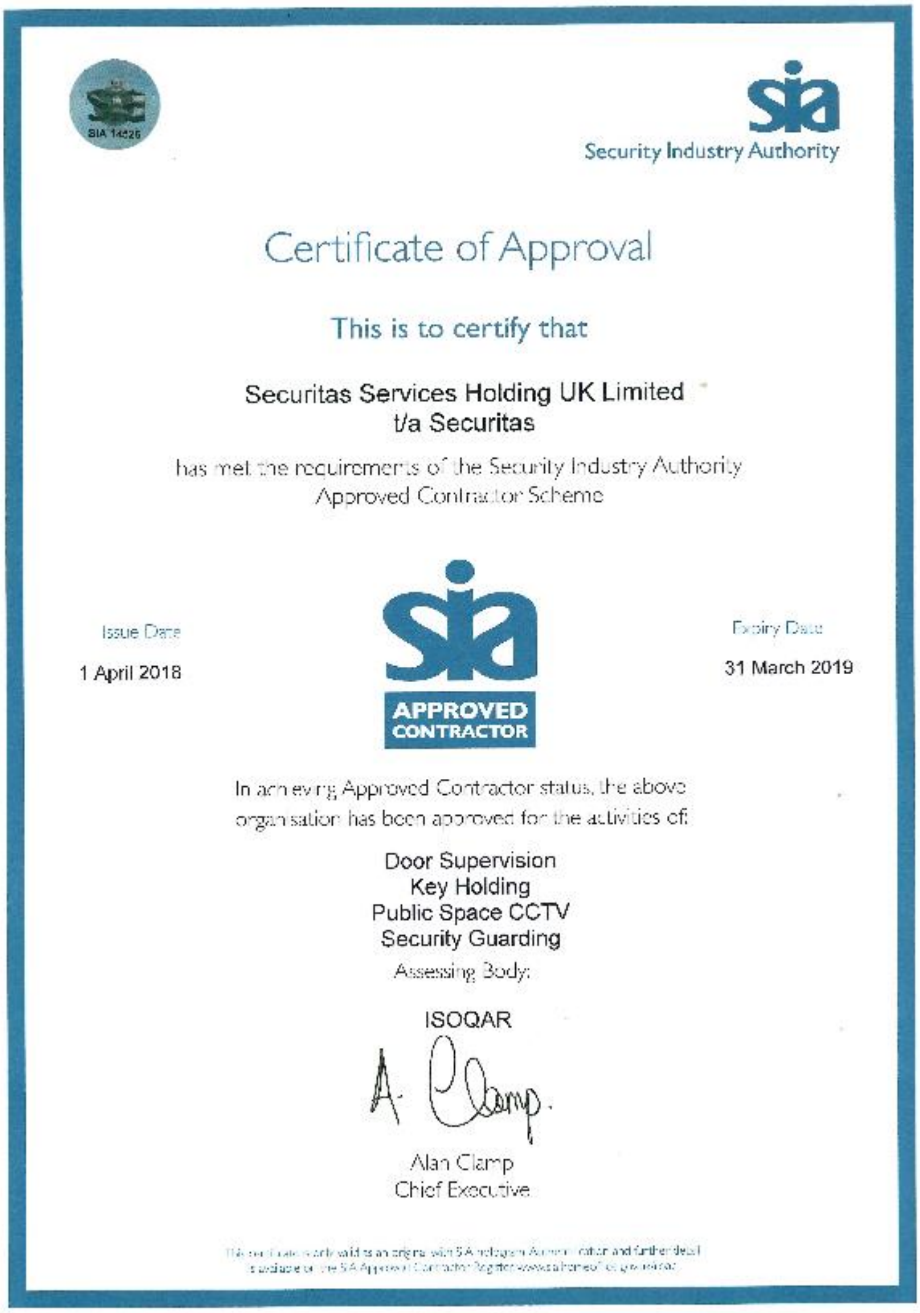
Scope of Registration:

The provision of manned security services including uniformed static guards, guard control systems incorporating a national communications centre, in accordance with the requirements of BS 7499, BS 7858, BS 7984 and BS 7958 Annex C.
The provision of an Alarm receiving Centre, monitoring services and alarm response in accordance with IS 228.

Signed:
Steve Stubley, Technical Director
(on behalf of Alcumus ISOQAR)

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by Alcumus ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting Alcumus ISOQAR. This certificate is one of several issued to registration number 3360.

Alcumus ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com W: www.alcumusgroup.com/isoqar
This certificate is the property of Alcumus ISOQAR and must be returned on request.



SIA 14526

Security Industry Authority

Certificate of Approval

This is to certify that

Securitas Services Holding UK Limited
t/a Securitas

has met the requirements of the Security Industry Authority
Approved Contractor Scheme

Issue Date
1 April 2018

APPROVED
CONTRACTOR

Expiry Date
31 March 2019

In achieving Approved Contractor status, the above
organisation has been approved for the activities of:

Door Supervision
Key Holding
Public Space CCTV
Security Guarding

Assessing Body:

ISOQAR

A. Clamp.

Alan Clamp
Chief Executive

This certificate is only valid as an original with SIA hologram. Authentication and further detail
is available on the SIA Approved Contractor Register www.sia.homeoffice.gov.uk/acs