SECURED BY DESIGN
ALARM STANDARD
Technical Guide June 2020

Secured by Design

SBD

Official Police Security Initiative

Contents

Introduction

Secured by Design (SBD) is part of Police Crime Prevention Initiatives (PCPI), a police owned organisation that works on behalf of the Police Service to deliver a wide range of crime prevention and demand reduction initiatives across the UK, and bring organisations together to create safer communities.

PCPI provide the Secretariat to the National Police Chiefs' Council (NPCC) Security Systems Group to monitor police strategies and technical developments and advise on policy requirements. PCPI also provide support to police forces and the private security industry on the administration of police response to security systems, including intruder alarms.

PCPI work with the national alarm inspectorate bodies and trade organisations for the security industry – the National Security Inspectorate (NSI), the Security Systems and Alarms Inspection Board (SSAIB), the Fire and Security Association (FSA) and the British Security Industry Association (BSIA) – to develop a partnership approach with the private security industry, specifically to improve the performance of security systems and increase the preventative impact and detection rate emanating from such systems.

Due to PCPI's technical intervention and the unified approach by police forces, there has been a decrease of over one million false calls to the police due to faulty equipment or user error. When set against a backdrop of an increase of 796,078 registered alarms in 1995 to 1,407,380 in 2019, this represents a significant reduction in demand on police forces.

Following increasing industry interest, PCPI has created a new SBD Alarm Standard for alarm installation companies that will provide a high quality alarm system and reduce false calls. The new standard is not a replacement for the NPCC Security Systems Policy or an alternative for certification by a UKAS accredited certification body - currently delivered by the NSI and SSAIB – but incorporates the existing criteria whilst building on police and industry knowledge and expertise to produce the new enhanced SBD Alarm Standard.

The SBD Alarm Standard has been introduced to further reduce false calls and to provide an alarm system of an enhanced quality. Installers meeting the SBD Alarm Standard now have the option of joining the new SBD scheme, following an assessment from their respective Alarm Inspectorate body, enabling buyers to have confidence in installers utilising the trusted 'Police Preferred Specification' branding.

Our team of Development Officers will help guide you through the process of gaining membership and explore with you the advantages of becoming a police recognised alarm system installer.

For more information visit: https://www.policesecuritysystems.com
or contact your nearest SBD Development Officer
https://www.policesecuritysystems.com/contact-us

1 Company requirements for SBD Alarm Systems

1.1 Trading

1.1.1 Companies will be required to have been compliant with their home police force for a minimum period of 2 years.

1.2 Sales

1.2.1 The company shall not sell SBD systems by cold calling by telephone or by door to door trading.

1.3 Training

1.3.1 Personnel involved in the design, installation, commissioning and maintenance of the alarm, shall hold industry recognised qualifications and competencies, e.g. NVQ Level 2, Certified Technical Security Professional (CTSP) or, Fire, Emergency and Security Systems (FESS) Level 3 Apprenticeship Standard.

1.3.2 All end users shall be fully trained in the use of the alarm system in accordance with Annex A.

1.4 Procedural

1.4.1 Remote restores, sometimes known as remote resets, are not allowed under this standard. Resets are to be completed on site by an engineer only.

1.4.2 Following commissioning and handover, all systems will be subject to a 14 day soak test period before a police response is requested by the Alarm Receiving Centre (ARC).

1.4.3 Engineers must place the system on test with the ARC when they arrive on site and remove from test when they leave. No alarm activations shall be sent to the police during that period unless accompanied by an audio-visual confirmation or a duress code.

1.4.4 Two or more false alarms in a rolling 12 month period resulting from engineering errors may result in the licence for an individual system being removed. Accidental engineer-sourced and user false alarm activations will count towards this total.

1.4.5 A company that has over a 50% false call rate may have their SBD licence removed.

Note: Performance of SBD alarm systems will be monitored by the police for compliance and reliability.

2 Technical requirements for a SBD Alarm System (Residential)

2.1 Standards and Grades

2.1.1 All alarms to be compliant with ‘PD 6662

Scheme for the application of European Standards for intruder and hold-up alarms', and only certificated equipment is to be used.

2.1.2 The minimum requirement is a Grade 2 alarm system but to include anti-masking properties.

2.2 Signalling

2.2.1 Systems will have dual path signalling to Dual Path 2 as a minimum.

2.3 Hold-up Alarms

2.3.1 Exposed cables for hold-up alarm buttons should be physically protected by ducting, conduit or trunking.

2.3.2 Where there is no hold-up facility on the premises, hold-up signals on the Alarm Transmission System (ATS) should be prevented.

2.4 Power

2.4.1 Mains failure must be adequately managed by providing a stand-by power source to allow for a minimum 24hrs supply.

2.4.2 Mains failure must also be signalled to the ARC and keyholders notified immediately.

2.5 Confirmation Hold-Up Alarm

2.5.1 Confirmation of such a signal is required and is to be based on a risk assessment of the premises and occupants, and may be:

i) Video

ii) Audio

iii) Sequential

2.6 Confirmation of Intruder Alarms

2.6.1 Two methods of confirmation are required based on a risk assessment of the premises and occupants, i.e.

i) Sequential and video

ii) Sequential and audio

iii) Audio and video

2.7 Opening Contacts

2.7.1 All perimeter doors are to have a contact fitted.

2.8 Setting and Unsetting

2.8.1 Setting and unsetting with a remote device controlled from a distance by the use of radio or electronic signals (e.g. mobile phone) is not permitted.

3 Technical requirements for a SBD Alarm System (Commercial)

3.1 Standards and Grades

3.1.1 All alarms to be compliant with 'PD 6662 Scheme for the application of European Standards for intruder and hold-up alarms, and only certificated equipment is to be used.

3.1.2 The minimum requirement is a Grade 2 alarm system but to include anti-masking properties.

3.1.3 BS 8243 Installation & configuration of intruder and hold up alarms designed to generate confirmed alarm systems, unsetting options 6.4.2 & 6.4.3 are permitted only, BS 8243 6.4.2 - Prevention of entry to the supervised premises before the intruder alarm system is unset.

BS 8243 6.4.3 – Prevention of entry to the supervised premises before all means of intruder alarm confirmation is disabled.

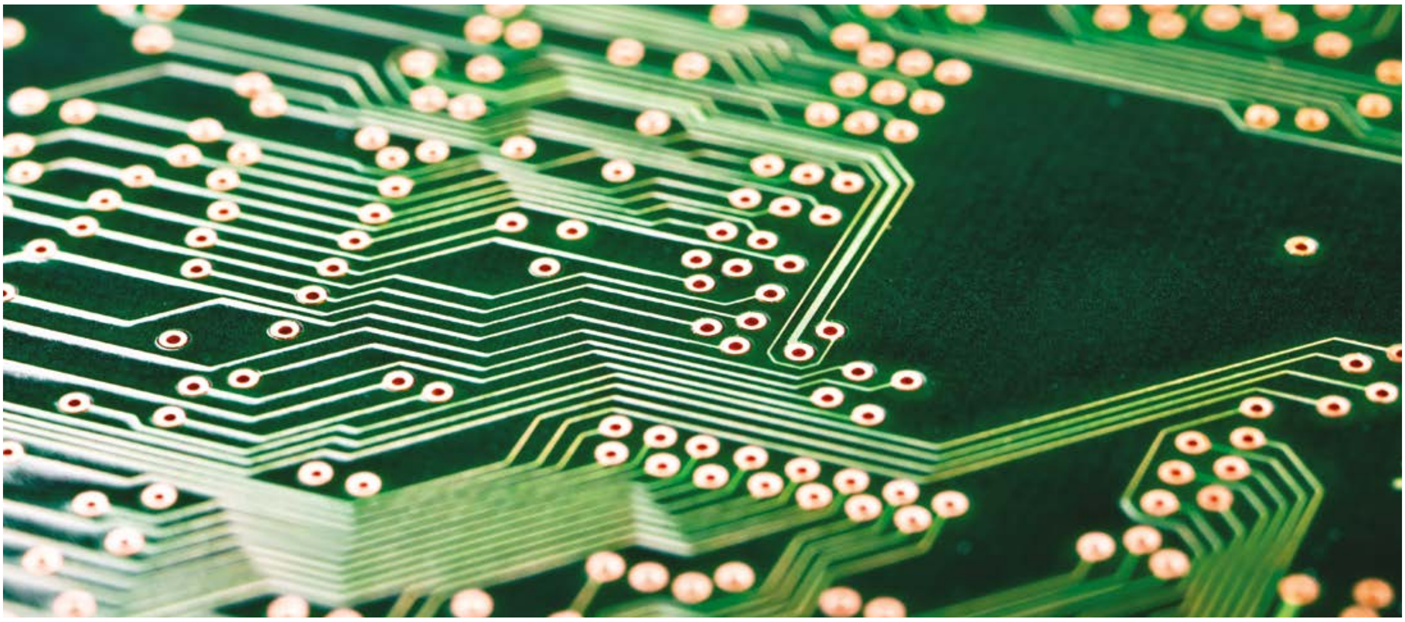
3.2 Signalling

3.2.1 Systems should have dual path signalling to Dual Path 2 as a minimum.

3.3 Hold-Up Alarms

3.3.1 Exposed cables for hold-up alarm buttons should be physically protected by ducting, conduit or trunking.

3.3.2 Where there is no hold-up facility on the premises, hold-up signals on the



Automatic Transmission System (ATS) should be prevented.

3.3.3 Hold-up alarms from any part of the system that is set, should not result in a police response.

3.4 Power

3.4.1 Mains failure must be adequately managed by providing a stand-by power source to allow for a minimum 24hrs supply.

3.4.2 Mains failure must also be signalled to the ARC and keyholders notified immediately.

3.5 Confirmation of Hold-up Alarm

3.5.1 Confirmation is required and is to be based on a risk assessment of the premises and occupants and may be:

i) Video

ii) Audio

iii) Sequential

3.6 Confirmation of Intruder Alarms

3.6.1 Two methods of confirmation are required based on a risk assessment of the premises and occupants, i.e:

i) Sequential and video

ii) Sequential and audio

iii) Audio and video

3.7 Sub-systems

3.7.1 Sub-systems must have adequate safeguards to ensure staff cannot enter protected areas while alarmed, e.g. electronic door locks linked to the system and turning it off prior to staff entering.

3.8 Setting and Unsetting

3.8.1 Setting and unsetting with a remote device controlled from a distance by the use of radio or electronic signals (e.g. mobile phone) is not permitted.

Annex A

User Training Requirements

1. Setting and unsetting of the alarm system.
2. Alarm abort procedure, including passwords.
3. Checking all perimeter doors and windows are closed and secure.
4. Correct use of the hold-up alarm system in accordance with NPCC Policy.
5. Keeping a record of alarms and engineer visits.
6. How to conduct a regular user walk test.

NPCC Security Systems Group Contacts

Ken Meanwell

Staff Officer

NPCC Security Systems Group

T: 07770 237173

E: ken.meanwell@police-cpi.co.uk

David Mair

Technical Representative

NPCC Security Systems Group

T: 020 7230 0749

E: david.j.mair@met.pnn.police.uk

NPCC National Police Chiefs' Council | SECURITY SYSTEMS POLICY

PCPI

Police Crime Prevention Initiatives

Secured by Design

SBD

Official Police Security Initiative

Police Crime Prevention Initiatives

1st Floor
10 Victoria Street
London
SW1H 0NN

T: 0203 8623 999
E: enquiries@police-cpi.co.uk
W: https://www.policesecuritysystems.com/