Risk Management Guidelines

General System Guidelines for New Intruder Alarm Installations in Commercial Premises

Introduction

Intruder Alarm Systems installed in the UK since 1st October 2005 are required to be designed, fitted and maintained in accordance with British Standards Institution (BSI) document PD6662:2004. Systems that are designed to generate confirmed alarm conditions are further subject to BSI document DD 243:2004. These two documents establish minimum standards for intruder alarm systems in buildings (whether commercial or domestic).

They do not, however, adequately address all of the features that insurers normally require of an alarm which is intended to protect commercial premises, and it is therefore necessary to give additional specification requirements to alarm installers when purchasing a new system.

Please therefore ensure that you pass a copy of these Risk Management Guidelines to your intruder alarm company and that they confirm that your alarm will comply with the following System Requirements.

Please also ensure that arrangements are in place to meet the requirements listed under the Keyholder Response section below.

System Requirements

Where intruder alarm protection is a condition of cover with RSA, the system should, unless otherwise expressly agreed, be installed in accordance with the following provisions:

1. Installation

1.1. The alarm system must be installed and maintained by a company which is recognised as an installer of intruder alarms by either the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB). It must also be recognised as a Compliant Company by the relevant responding police force. Remote signalling (if incorporated) must be to an Alarm Receiving Centre which is inspected and certified by NSI or SSAIB.
(Please note that in some circumstances, a more restricted selection of installation, maintenance and / or monitoring companies may be warranted).

2. Control Equipment

2.1. Except for ancillary control equipment (such as remote keypads and PACE readers), control and signalling equipment must be located in a position where it is concealed from general view and is least vulnerable to attack.

3. Setting / Unsetting

3.1. The means of unsetting the system described in paragraph 6.4.4 of DD 243: 2004 (whereby opening the initial entry door will disable all means of alarm confirmation throughout the protected premises) must not be employed.

Risk Management Guidelines

4. .Warning Devices

4.1. Audible warning must be by either two external self-actuating audible warning devices OR by one external self-actuating warning device and an internal self-actuating siren or two tone electronic sounder, each giving a sound emission of at least 100dB at 1 metre.

4.2. Where it is not possible to install an external warning device above 3 metres (i.e. so that it would not be readily reached from ground level), two external self-actuating warning devices must be fitted. They should be sited on different elevations of the premises if at all possible.

4.3. All warning devices must be instantaneous in operation unless:

- a delay is required by the local Police Force Intruder Alarm Policy in which case the delay shall be for the minimum duration specified in that Policy and clearly stated in the intruder alarm specification (system design proposal)
  or
- an audio confirmation alarm system is installed.

4.4. Any such delay must be automatically removed in the event of loss of remote signalling capability or withdrawal of police response. This applies irrespective of the method of confirmation (if any).

4.5. Where the system has remote signalling, any internal warning device must be sited remotely from the control panel so as not to identify the position of the panel when activated. For the same reason, any internal sounders used as part of the alarm setting / unsetting procedure must also be sited remotely from the control panel.

5. Detector Equipment

5.1. Preference should be given to the use of equipment appearing on the current LPCB list of approved products and services if suited to the purpose.

5.2. When the system is in test mode only it shall be possible for one person to check the area of detection of all movement detectors.

Risk Management Guidelines

6. Confirmable Alarm Systems

The following paragraphs 6.1 to 6.6 only apply if the intruder alarm is to be a confirmable system.

6.1. The whole system to be designed and configured such that when an intruder enters any part of the protected premises there is a high degree of certainty that the alarm system will deliver a confirmed alarm message.

6.2. Signalling must be via an acceptable dual-signalling system such as RedCARE GSM, DualCom Plus or DualCom GPRS G4.

6.3. Following the cancellation of an alarm signal the system must re-arm without any zone, sensor or detector being locked out so that the whole system remains alert to signal further alarm information during the set period.

6.4. To prevent tampering once the system has been set, all microphones and cameras intended for confirmation purposes must be located within areas covered by intruder alarm detection devices.

6.5. All control and remote signalling equipment other than ancillary control equipment (such as remote keypads and PACE readers) must be located so that it cannot be accessed whilst the alarm is set without creating a confirmed alarm condition.

6.6. The alarm specification (system design proposal) must include the actions to be taken by the alarm receiving centre upon receipt of the following alarm messages or information:

- a confirmed alarm condition (including circumstances where the loss of one or more signalling paths contribute to the confirmation criteria)
- an unconfirmed alarm condition (including any variations according to whether or not the system can be rearmed in its entirety)
- a telecommunications failure (including the failure of one telecommunication path in a dual-path signalling system)

Risk Management Guidelines

Keyholder Response

Remote signalling systems must be allocated a police Unique Reference Number (URN) and thus benefit from police attendance to alarm activations in accordance with the Force Policy on Response to Security Systems. If there is notification of a reduced level or withdrawal of Police response to the system, RSA must be informed immediately.

The premises must not be left unattended unless physically secured and the alarm system is fully set including the designated methods of remote signalling.

If the alarm is activated (whether the activation is confirmed or not), or any signalling path is lost, the appointed key-holder must attend the premises immediately to investigate the reason for the activation. If there is a fault with the alarm system or an alarm signalling path, an engineer should be called and the keyholder should not leave the premises unattended until they are fully re-secured, with the alarm system and its signalling paths fully reset.

Failure to both fully secure and alarm the premises may invalidate your insurance cover.

Risk Management Guidelines

These and other Risk Management Guidelines addressing a wide variety of risk control issues are freely available from:

http://www.managerisk.rsagroup.co.uk

The information set out in this document constitutes a set of general guidelines and should not be construed or relied upon as specialist advice. Therefore RSA accepts no responsibility towards any person relying upon these Risk Management Guidelines nor accepts any liability whatsoever for the accuracy of data supplied by another party or the consequences of reliance upon it.