ASTONLARK

RISK MANAGEMENT

# General Security Recommendations for Commercial Premises

## INTRODUCTION

Your assets and your business are at risk from criminal damage, burglary, and catastrophic arson attack. In some circumstances, the lives and safety of your employees are in jeopardy from the actions of criminals.

Whether you are planning the construction of a new building, moving into new premises, refurbishing an existing site, considering the enhancement of protections following unauthorised entries or in response to a particular crime threat, or just taking a fresh look at your safeguards, it is essential that the standards of physical, electronic and other security precautions you select are at levels commensurate with the risk.

This information sheet has been prepared to assist you in determining the level of security required. It is broken down into three sections: physical, electronic and manned security.

Additional guidance on the correct standards of physical, alarm, manned security or other protective measures can be provided by the local Police Crime Prevention Officer.

## PHYSICAL SECURITY

The physical security of any site has three distinct aspects, the perimeter protection to the site, the external protection of the buildings and specific protection to vulnerable areas or theft of attractive contents.

## 1.1 FENCES, GATES, BOLLARDS AND SECURITY LIGHTING

### FENCES

The importance of suitable perimeter fencing as the first line of defence cannot be understated. The openness of many sites renders them highly vulnerable to intruders.

The boundary to open sites should be protected by security fencing and gates, which conform to BS 1722. Check with your planning authority to determine whether permission is required to erect fencing.

Many different types of fencing are commercially available and the fencing selected should not hinder external surveillance by providing a shield to the intruder's activities.

- Timber fencing has very little real security value and often impedes surveillance. The use of such fencing in a commercial environment should be avoided.
- Quick thorn hedges should only be used to supplement the security provided by other fencing.
- Chain link fences are easily distorted or cut and do not constitute a very effective barrier. They should be avoided in areas of high risk.
- Weld mesh or expanded metal fences are effective against all but the most determined of intruders and are available in a range of gauges and strengths. Weld mesh is suitable for many commercial security applications.
- Steel palisade fencing presents a very substantial barrier. Vandal resistant rivets, shear bolts and saddle head bolts should be used in the installation to prevent removal of sections. The tops of each vertical section should be multiple barbed for ultimate protection. Palisade fencing is suitable for many commercial security applications.

- Fence heights should not be below 1.8m. However, to have real security value they should be to a height of 2.4m.
- Barbed wire, barbed tape and other enhancements can be strung between the outward cranks at the top of fence posts, to increase fence heights and enhance security. The use of barbed wire on lower fence areas readily accessible to the general public is not recommended in view of its potential hazard to cause injury.
- Fences should be fixed to a concrete base foundation to prevent lifting and under crawling.
- Improved security can be provided by alarming the fence.
- Power fences used as a supplement to good quality perimeter fencing offers significant additional protection (consult Lark (Group) Limited for full details).

## GATES

- Gates should be regarded as a continuation of the fence and must be of equivalent strength, security and height to the fence.
- As wide gates are more difficult to secure than narrow ones, gates should not be wider than their usage demands. Double gates can be used subject to the following being taken into consideration:
- Adequate locking bolts being used on the dead leaf (first closing leaf) of the gates.
- Securing with a padlock on the inside through permanent hasps and staples. Chains should not be used with padlocks, as they are weak points and, also usually allow unwanted movement between the closed leaves.
- Gates must be secured by heavy duty close shackle padlocks having a minimum of 5 lever or 6-pin tumbler operating mechanisms.
- Hinge pins to gates should be reversed, reverted, pinned, burred, welded or suitably defaced to prevent gate removal by lifting off the hinges.

Turnstiles are a most effective way of controlling pedestrian movement in and out of premises.

Designs are available in single or multiple form with non-reversible one way and bi-directional revolving units. They can be manual, card or remote control operated and are also lockable.

## BOLLARDS

Fixed or telescopic steel bollards or posts should be installed to protect any vulnerable perimeter areas, vehicle parking areas or where there is an identified risk of "ram-raids" (consult Aston Lark Limited for full details).

## SECURITY LIGHTING

On conspicuous or manned sites effective security lighting of external areas can be a valuable additional precaution in the fight against criminal activity. Well-sited lighting of the right intensity is essential to provide a satisfactory level of protection.

Security lighting also has some potential disadvantages if not competently installed. A poorly designed lighting installation can, in fact assist the vandal or thief by providing light to work with and shadows to hide in.

Lighting systems are only effective if switched on at the appropriate times. An automatic form of control (photo-electric cell, time switches or movement activation by infra-red sensors) is usually the best option.

All elevations including recessed areas that benefit from casual surveillance from occupied neighbouring property or passers-by should be illuminated by security lighting during hours of darkness.

A combination of movement activated lighting, linked to an external audible alarm system can be a significant deterrent.

## 1.2 DOORS, WINDOWS AND SKYLIGHTS

### DOORS

All external doors should be of solid-core construction and of at least 44mm thickness.

- Restrict the number of external doors to the minimum required to carry out your business and to conform with the fire regulations.
- While manipulation and lock picking is now a rare occurrence, every attempt should be made to defeat such attempts by the choice of best quality mortise deadlocks (carrying the BSI kite mark) having a minimum of 5 lever of 6 pin-tumbler operating mechanisms and box steel striking plates of complimentary strength.
- Avoid the use of 'night latches', which are easily 'sprung'.
- Fire exit doors and all other outward opening doors should be fitted top and bottom with hinge bolts (dog bolts). This offsets the vulnerability of these doors due to the exposed hinges and prevents door removal even if the hinge pins are attacked.
- Doors which are vulnerable to attack should be faced on the exterior surface with 16 gauge sheet steel, secured by non-return screws or with coach bolts and preferably wrapped round the door edges or overlapping the frame to prevent jemmy attack. The doorframe and fixings should be strengthened to take the extra weight. Alternatively doors approved by the LPCB: - Loss Prevention Certification Board, to Loss Prevention Standard LPS1175 grade 4 (or better) should be considered.
- Ideally, large vehicle type doors and shutter doors should be secured internally with substantial locking bar and heavy duty close shackle padlocks having a minimum of 5 lever or 6 pin tumbler operating mechanisms. Alternatively shutter doors should be secured by two proprietary key operated shutter bolts, one into each of the side guide rails/channels.
- Some additional security for electrically operated roller shutter doors can be achieved by securing their power isolating control switches in the off position by good quality padlocks. Whereas, chains to manually operated shutters should be secured to the lug of their wall brackets using good quality padlocks.
- The best way to protect recessed porches is with the installation and use of durable steel roller shutters approved by the LPCB: - Loss Prevention Certification Board, to Loss Prevention Standard LPS1175 grade 4 or better.
- Glazing in doors should, where possible, be avoided. If glazing is required then it should be of 7.5 mm (minimum) laminated glass in a panel not exceeding 100mm x 150 mm in dimensions. Beading should always be pinned internally to the door and ideally, suitable internal metal grilles or bars fitted.

### WINDOWS AND SKYLIGHTS

- As a minimum, all basement, ground floor, and other opening windows/ skylights accessible without the use of a ladder should be fitted with best quality key operated window locks (with detachable key).
- Where windows are not required to be opened they may be permanently screwed or bolted shut as an alternative.
- Opening windows that are over 900 mm in width or height should be fitted with a minimum of two key operated window locks.
- Internal steel grilles or shutters (approved by the LPCB: - Loss Prevention Certification Board, to Loss Prevention Standard LPS1175 grade 4 or better) or bars should be considered and are essential in areas where there are theft attractive contents, vulnerable windows or a history of unauthorised entries.

- If bars are fitted it is recommended that they are of solid mild steel of at least 18 mm in diameter and spaced at 125 mm centres with horizontal tie bars not more than 600 mm apart.
- All sections/panels of glass in louvered windows should be securely fixed with suitable adhesive into their brackets.

## 1.3 COMPUTERS AND MONEY

### COMPUTERS

Due to constant technological advances and the demand for ever more sophisticated processing capabilities, the cost of computer (and other electronic office equipment) theft and consequent business interruption, is a major concern.

- Experience has shown that the implementation of a combination of counter measures (along the lines of those specified in this information sheet) is invariably the only defence against crimes of this nature.
- Time is the thieves enemy and an immediate benefit accrues if the target property (i.e. computers, keyboards, VDUs, printers and facsimile machines) is located at least 2 metres away from perimeter glazing. Ideally all computers should be located on upper floors.
- Central processing units, file servers and tower computer systems should not be visible to passersby. Window blinds should be put into operation at the end of each working day or the use of one-way glazing, reflective foil or opaque film considered.
- All computer hardware and target property must be prominently and permanently security marked with the company name and area postcode. Warning notices should be prominently displayed on perimeter doors and windows drawing attention to the fact that the property has been security marked. Marking should be of such size and in such a position that its existence cannot be over looked and its removal or concealment would prove very difficult.
- The most effective security device in combating the removal of target property and their components is the "entrapment" security enclosure. Target property on site should be protected by security enclosures satisfying the requirements of LPS (Loss Prevention Standard) 1214 Issue 2 Category 2.

### MONEY

Cash (including luncheon vouchers & gift vouchers) is obviously a very attractive target for criminals and its presence, even in moderate quantities, can pose a threat to the building and its occupants.

Cash levels should be kept to a minimum and cash should never be kept on the premises for a moment longer than absolutely necessary. At no time should it be left unattended or handled, in an area visible to visitors, the public or members of staff at large.

Wages and salaries should be paid through banks or by cheque.

If considerable quantities of cash are regularly handled an adequate safe should be installed.

Where very large amounts of cash are handled, a secure cash office should be erected. We will be pleased to supply a suitable specification on request. The use of panic or personal attack alarms would also be needed in such areas.

The make and model of safe chosen should be suitable for the maximum amount of cash expected to be held. The safe should be approved by the Loss Prevention Certification Board (LPCB) to the relevant security grade of Loss Prevention Standard LPS1183. Details of any alternative safe not complying with LPS1183 must be referred to Lark (Group) Limited for approval, prior to purchase and installation.

The following measures should be observed in respect of burglary safes:

- All safe combination numbers should be removed from the premises out of normal working hours. The numbers chosen should be completely random and have no connection with personal details of staff. Under no circumstances should combination numbers be written on nearby walls or on the safe itself.
- All safe keys/key bits should be removed from the premises out of normal working hours. Under no circumstances are safe keys to remain on the premises when the building is unattended.
- The safes should be anchored in accordance with the manufacturer's recommendations and an installation certificate provided to this effect.
- Where an intruder alarm system is installed it is advisable to fit the safe with a limpet vibration detection device linked into the alarm.
- Where there is a hold-up danger the safe should have a deposit chute and be fitted with a time delay lock to prevent opening for a period of up to 30 minutes.

Where considerable quantities of cash are stored, the safe may be required to have an additional locking mechanism.

To minimise the quantity of cash in transit, daily banking is preferable. A professional security collection company satisfying the requirements of BS7872 should be used for the transportation of large amounts of cash. Where cash has to be transferred by employees, the following safeguards should be employed:

- The moments of greater risk in cash transportation are when leaving the building and arriving at the bank. Wherever possible cameras from any CCTV system on your premises should be used to monitor cash handling and transportation activities on site.
- Full training should be given to those persons who will be accompanying the cash carryings, including instructions not to place themselves in danger.
- The route and time of collections and deliveries should be varied on each occasion.
- The transit of cash should be by vehicle, and ideally the doors should be locked at all times. The vehicle used should also be varied as often as is practicable.
- The routes should avoid isolated or known trouble areas and should keep too busy thoroughfares and main roads.
- Park the vehicle as near as is possible to your premises and the bank.
- A mobile phone or two-way radio should be provided. This should have a one-button operation dial the emergency services.
- Before getting out of the vehicle, check the surrounding area for anything suspicious and alight where there are a large number of people around.
- Money in transit should be accompanied by a minimum of two able bodied, adult employees (refer to your insurance policy).
- Ideally proprietary cash spoiling devices/bags should be used.
- If substantial amounts of money are being carried then consideration should be given to splitting the money into different cash carrying bags, or preferably, separate journeys made.

## ELECTRONIC SECURITY

There are many benefits of an electronic security system. Firstly its mere existence will act as a significant deterrent to intruders. Secondly it will assist in the early detection of intruders and will thus restrict the amount of time available to an intruder and hopefully minimise any losses. Finally electronic security systems can also assist in the apprehension of intruders.

### 2.1 INTRUDER ALARMS

The premises should be protected by an Intruder Alarm System designed, installed and maintained in accordance with the provisions of BS4737: Intruder Alarm

Systems in Buildings or BS EN 50131-1:2006+A1:2009.

1. General Requirements for Intruder Alarms; and shall meet the requirements of the relevant Police Inspectorates or Force Polices. The Alarm System must be installed and maintained by a company which is acceptable to the local Policy Authority.

Protection coverage should comprise of (at least) magnetic reed contact switches upon all external doors and suitable internal volumetric movement detection throughout.

## CONTROL EQUIPMENT

The system shall be designed to record and store the events defined in the next paragraph, which have occurred within the last 30 days. The record to include the time and date of each event; more than 3 consecutive events of the same condition need not be recorded within an alarm set period.

- Events for recording purposes shall include setting, unsettling, reset, any activation, fault, isolation or an inhibit of any part of the system, transmission failure, tamper conditions, valid user codes, alterations to clock and software and loss of mains power.
- Where the number of recordable events during a 30 day period is likely to exceed 100, the system shall be capable of recording a minimum of 200 events, producing a hard copy record of events when requested.
- The event records must be retained for at least 30 days in the event of a power failure.
- Event recording may take place at the control panel and/or at a remote location.
- The completion of the setting procedure shall be achieved by the operation of a key-operated shunt lock fitted to the final exit door, or by the operation of a push button final exit set switch or ferrous key fob mounted outside the protected premises, adjacent to the final exit door.
- Time delays incorporated into the entry route shall be kept to a minimum to allow entry/exit without causing false alarms. A possible way of achieving this will be by use of Type A remote keypads (those in which processing of the code is not carried out) in conjunction with the main alarm control panel located in a secure area. The total delay including secondary timers when used must not exceed 45 seconds.
- For a system incorporating remote signalling, set and unset signals shall be transmitted to and logged at the alarm-receiving centre.
- Detectors incorporated into the final exit route should create an alarm condition if their activation is not preceded by the initiation of the correct unsetting procedure.

## WARNING DEVICES

External warning devices shall have the mechanism and circuits enclosed within a metal housing sited at least 3m off the ground or out of normal reach. Where this cannot be achieved, two self-actuating warning devices must be installed.

- The external warning device must be designed to resist the injection of foam. Alternatively the device shall have facilities to detect the presence of foam.
- Any delay on audible warning devices shall be in the minimum acceptable to the responding Police Authority and clearly stated in the Alarm Specification.
- Where the system has remote signalling an internal warning device shall be sited remotely from the control panel so as not to identify the position of the panel when activated.
- Strobe lights shall operate concurrently with audible warning devices.

## DETECTORS

Preference should be given to the use of equipment appearing on the current LPC list of Approved Products and Services if suited for the purpose.

- In areas where there is a possibility that detectors could be subject to compromise (e.g. unsupervised access by members of the public), consideration should be given to use of detectors incorporating anti-masking features.
- 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.
- Alarm confirmation Systems which are designed to provide confirmation of alarm signals to alarm receiving centres should comply with requirements of BS DD243 2004 "Intruder Alarm Systems Signalling to Alarm Receiving Centres"

## REMOTE SIGNALLING

The system should be designed to signal to a Central Monitoring Station via the BT Redcare/GSM, CSL DualCom GPRS Grade 4 or an IP dual signalling system that has been certified by the Loss Prevention Certification Board (LPCB) as LPS1277 Issue 3 compliant, operating at performance level ATS5 and installed in accordance with ANNEX C of the standard or other signalling systems approved by Aston Lark Ltd

- All central stations used in connection with alarm signalling must be approved by NSI as meeting the requirements of BS5979: 2000 "Code of Practice for Remote Centres Receiving Signals from Security Systems".
- All telecommunication lines used for alarm signalling must wherever possible enter the protected premises underground or in a manner which is unlikely to render them liable to attack.
- All telecommunication lines used for alarm signalling should be subject to BT's "Totalcare" maintenance service (i.e. 24 hour response 7 days a week).
- Audible and visual indication of a line fault condition must be provided at the control panel when the alarm system is unset. In addition, when a line fault condition occurs it must be logged and handled by the control panel in the appropriate manner.

## 2.2 ACCESS CONTROL

Many losses in commercial and industrial premises occur during business hours.

Access control systems may stand alone to control access via a single entrance or may be programmed to allow different levels of access to different people in different places at different times. In premises where a large number of employees work and/or there are several points of entry/exit, the provision of an access control system is advisable to reduce the risk of unauthorised access.

The following are some basic guidelines to help you manage access control but ideally it would be beneficial to install a mechanical or digital access control system, proximity card system or videophone entry system to the main points of entry/exit to prevent access by non-staff members.

- It is important to restrict entry to as few locations as possible.
- A visitor-monitoring scheme should be introduced. Visitors should be required to sign in and sign out when leaving the premises. All visitors on the premises should be issued with badges that include their name and the date of issue. All staff should then be instructed to challenge any strangers not wearing official visitor badges.
- The main entrance into the building should be clearly signposted from both the pedestrian and vehicular

entrances, to ensure that all visitors report to the main reception area.
- The propping open of external doors by employees, either during periods of warm weather or for convenience of access must be discouraged.
- A reception area should be created by the main entrance point, with a secure lobby, which would contain a waiting area and restrict entry into the building until allowed by a member of staff.
- The visitor entrance door should be secured during the day, by at least the use of a latch type lock. A bell should be provided to call for staff attention.

## 2.3 CCTV

Closed Circuit Television Systems are a considerable deterrent and should be considered to complement other security measures. They are particularly beneficial when manned guarding is provided on site or when off-site monitoring is undertaken by the National Security Inspectorate (NSI) approved central monitoring station, meeting the requirements of BS5979.

- Closed Circuit Television Systems should be installed by a company recognised by NSI/ SSAIB and acceptable to the local police authority.
- CCTV systems should comply with all relevant British Standards and NSI/SSAIB codes of practice.
- Video recording facilities are strongly recommended, and are essential if no manned guarding or offsite monitoring is undertaken.
- Any video recorders need to be in a secure and suitable storage facility, which itself should be within a secure area e.g. permanently manned control room or protected by an intruder alarm system.
- A suitable number of tapes should be rotated to avoid erasing vital evidence. Police authorities recommend that video recording tapes be kept for a minimum of 28 days, before they are re-used. Tapes should be replaced after 12 months use.
- As an alternative to video recording, a digital recording system could be used.

## SECURITY PERSONNEL

Experience has shown that unattended or physically isolated sites are vulnerable to malicious damage. Surveillance involving a continuous site presence, regular patrol visits or remote surveillance using CCTV offers a significant deterrent against opportunist and professional crime.

The principal objectives of the security guard are to protect against:

- Unauthorised entry to the site and/or premises.
- Theft or malicious damage.
- Indiscipline by staff, contractors and visitors.

Vetting processes contained in BS7499 should be considered for persons to be employed on security duties whether using your own in-house security personnel or contract security personnel.

- Contract Security Personnel should be recognised by and registered with SIA (Security Industry Association)
- The site should be thoroughly patrolled on a regular (at least hourly) basis. Patrolling guards should have their movements check audited by means of mechanical or electrical clocking devices. The practice of entering the time of a patrol in a book is not a satisfactory method and is open to abuse.
- The guard should also be provided with a portable radio personal attack switch linked to the premises intruder alarm system to summon support in emergency circumstances.
- Guards should be based in a compartment outside of the areas protected by the intruder alarm system. Alternatively the system should be “zoned” to enable the

protection to the areas occupied by the guard to be “unset” when he/ she is in occupation, whilst the remainder of the system is “live”.

- Arrangements should be made with the alarm company Central Monitoring Station, to ensure that alarm activation’s are promptly communicated to the guarding contractor.

ASTONLARK



**YOUR WORLD IS OUR FOCUS**

**www.astonlark.com**

AL -RM-GSRCP-0718

Chartered
Insurance
Brokers