RiskFix

Balanced Risk Engineering Solutions

Unstaffed Extended Opening Hours

Local Authorities may wish to extend opening hours of libraries without incurring the cost of having employees on-site. Therefore an electronic solution may be implemented to allow restricted public access. This increases the risk of a potential loss; therefore some preventive measures must be taken.

This document is not meant to cover any issue relative to a casualty / liability insurance policy, but is purely orientated to property damage loss prevention.

Intruder alarms

Perimeter intruder detection is recommended with virtual barriers or infrared beams, etc.

Magnetic contacts to be provided on all doors. Both external doors and internal doors ensuring the separation between the public accessible areas and non-accessible areas must be fitted with magnetic contacts.

Glass break detectors to be fitted on all glazing walls, windows, etc.

Motion sensors such as passive infrared detectors must be fitted inside the building with total coverage.

All unoccupied areas must be fitted with an intruder alarm.

Intruder alarms must have been designed, installed and under maintenance contract including a twice-yearly service by a NSI Gold approved contractor. AIG minimum requirement is Grade 3 equipment and Grade 4 notification having a dual path monitored scheme to a NSI Gold approved Alarm Receiving Centre.

Employees access control system

An access control system must be implemented for the employees with personalised individual photo ID.

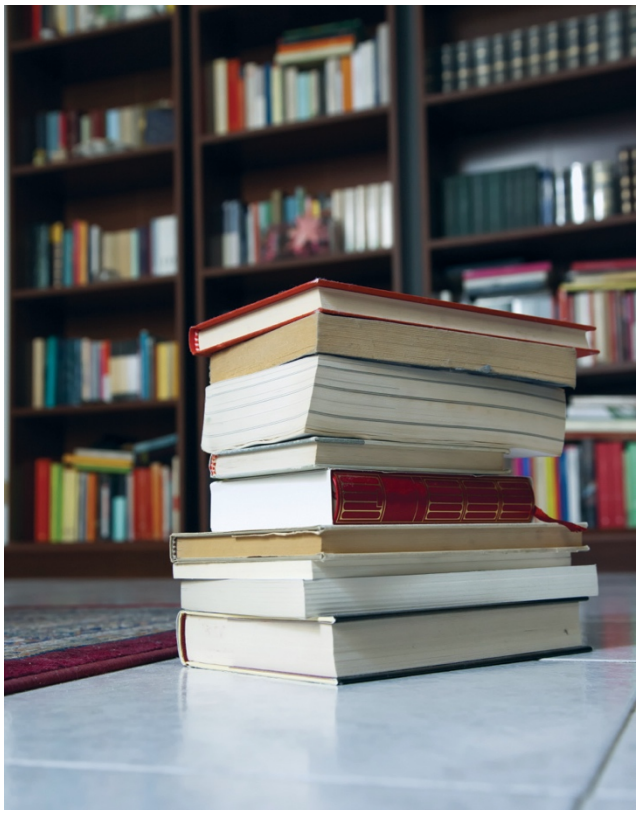
It must be fitted with an anti-pass-back system, so one badge cannot be swiped to re-enter the premises immediately or shortly after it has been validated for entry. A time-delay of 30 minutes should apply before allowing this card/person to re-enter the premises.

Automatic fire detection

Extensive internal automatic fire detection coverage must be provided in compliance with the latest enforceable edition of BS 5839 – type L1/P1.

Design, installation and maintenance must be completed by a LPS 1014 approved contractor.

A maintenance contract including a twice-yearly service must be signed.



Alarm & CCTV management

Alarm signal must be reported to a 24/7/365 manned alarm receiving centre NSI Gold approved. A formal procedure must exist to manage alarm signals.

CCTV should be remotely monitored permanently.

CCTV

Comprehensive internal and external coverage must be provided. The required standard is NACP 20 – CCTV Code of Practice.

CCTV should be digitally recorded for 30 days.

Design, installation and maintenance must be completed by an NSI approved company.

Adequate external lighting must be provided to allow good quality CCTV coverage during hours of darkness.

Cash management

Make sure there is no cash left in the premises during unmanned (meaning no library employees inside the premises) hours within public accessible areas. Safes must be anchored in the ground, under alarm with time delay devices, located in a concrete built room with CCTV, restricted access and access control. The maximum amount of cash held on site must not exceed the safe allowance (refer to Euro grade classification to BS EN 1143:2012).

The safe should be located in an approved intruder alarm protected area and should be anchored in accordance with the manufacturer's instructions.

The safe should be equipped with deposit facilities to allow cash to be regularly deposited without the need to open the safe and time locks to restrict opening of the safe.

The safe keys should be taken off site overnight.

Combination codes should not be written down and should be changed at least every six months.

The cash office construction should be compliant with BS EN 356 / BS EN 1063 and BS ENM 1522 / 1523 and be fitted with a 'silent' hold-up alarm and a 'duress code' for use if staff are forced by thieves to unset the alarm and specific opening / closing time monitored by the alarm receiving centre.

Material Accessibility

Rare or valuable books should not be accessible during unstaffed extended opening hours and should be kept safely locked in an under alarm area.

Electronic material management

Computers should be carefully sited within the premises, preferably above ground level, with no readily accessible windows.

Computer and self-service station must be secured with proprietary lockdown devices conforming to the appropriate Security Category of LPS 1214.

Laptops should not be left unattended at any time. If left in the premises they should be placed in a secure store or cabinet.

Extra-hours system access

The number of entrances to the premises must be limited to the minimum possible, ideally one.

It must be fitted with anti-pass-back system, so a badge cannot be swiped to re-enter the premises after it has been validated. A time-delay of 30 minutes should apply before allowing this card/person to re-enter the premises.

An Air-lock or similar system with interlocked doors to be provided to avoid tailgating.

Access badges must be personalised and individualised with photo ID and PIN Code. The system should lock down the user after three false attempts of the PIN code.

Young people (16 years old and under) must not be allowed inside alone.

Fix the management system main central panel on a wall in a fire-separated and dedicated room. It can be included in the IT room. It should not be connected to the public network to avoid hacking risk.

All electrical installations must be included in the regular fixed wired installation control, PAT tested and subject to infrared thermographic scanning.

Internal compartmentation

An approved separation space must be provided between out of hours public accessible areas and restricted areas. Doors must be locked and secured and provided with adequate anti-intrusion rating.

If only part of the normal public accessible area is open with this system, there must be a good separation between those areas.

Security Guard

Provision should be commensurate with the risk; the AIG best practice recommendation being at least two security guards permanently on site during extended opening hours. They must be licenced by the SIA and contracted from an NSI Gold approved company. As part of their mission they should complete random internal and external recorded rounds every hour covering the whole premises.

They should be aware of emergency procedures and required actions in the event of an emergency. They should provide detailed reports of any incident to a senior site manager.

Closing Procedure

The system should control and shutdown lighting, air-conditioning and heating in the accessible area.

The intruder alarm must be activated at closing time.

Doors must be locked and secured.

Confirmation that the building is empty of all members of the public by the security guard.

Standards

The references are the latest enforceable edition of:

BS EN 50132 - Alarm systems. CCTV surveillance systems for use in security applications

NACP 20 – CCTV Code of Practice; issued by the National Security Inspectorate (NSI).

BS 8418 – Installation and Remote Monitoring of Detector Activated CCTV.

BS 5979 – Code of Practice for Remote Receiving Centres for Alarm & CCTV.

BS 3621:2007+A2:2012 - Thief resistant lock assembly. Key egress

CEN EN 12320:2001 - Building hardware. Padlocks and padlock fittings. Requirements and test methods

BS EN 1143:2012 - Secure storage units. Requirements, classification and methods of test for resistance to burglary. Safes, ATM safes,strongroom doors and strongrooms

BS 5839: 2013 - Fire detection and fire alarm systems for buildings. Code of practice for design, installation, commissioning and maintenance of systems in non-domestic premises

BS 7499 – Code of Practice for Static Site Guarding and Mobile Patrol Services.

BS 7984 – Code of Practice for Key holding and Response Services.

Security Industry Association (SIA) licences for all appropriate security company staff. Some SIA compliant companies have joined the SIA non-compulsory Approved Contractor Scheme (ACS); however SIA licences are still required for individual security company staff.

Accreditation by the National Security Inspectorate (NSI) for guarding operations including compliance with the above standards.

BS EN 356 / BS EN 1063 – Resistance of Glazing to Manual / Ballistic Attack.

BS ENM 1522 / 1523 – Resistance of Structure to Ballistic Attack.

PD6662 – Scheme of Implementation of European Standards.

European Standard EN 50131 – Alarm systems, Intrusion and hold-up systems. System requirements.

European Standard EN 50136 – Alarm systems. Alarm transmission systems and equipment. General requirements for alarm transmission systems.

DD 243 - Code of practice for the installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions.

For further information please contact your local AIG Property Engineer

www.aig.co.uk