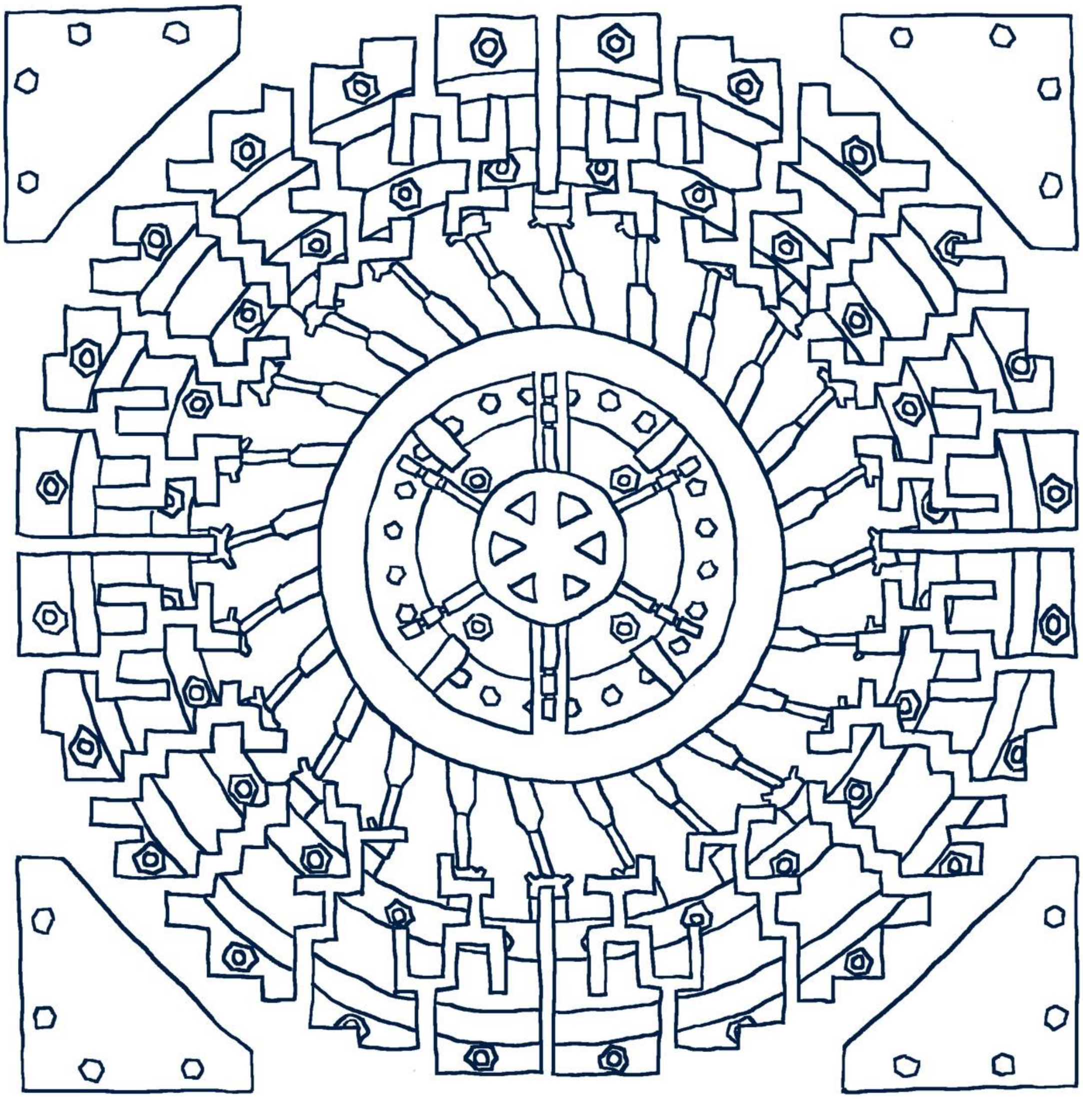
Estates Services
Crime Prevention Design Guide



Oxford University Security Services
The Old Observatory
South Parks Road
Oxford
OX1 3RQ
01865 272944

‘*Delivering Safety and Security through Prevention, Reassurance and Response*’

The University of Oxford - Security Services

Crime Prevention
Design Guide

Design & Layout
and
Physical Security

Incorporating soft landings for Security Services

Lesley Nesbitt **Ad Cert ED & CP**

Crime Prevention Design Advisor

Version Control Sheet for Crime Prevention Design Guide

Date	Version number	Reason for revision and by whom	New Version Number
2013/14	Draft	Draft document amended having received feedback from Lyndie Hayes, John Hewitt, Isobel Hughes, Steve Pearson, Nigel Aplin. External verification of document and security standards (Thames Valley Police). Revised to Version 1 by Lesley Nesbitt Security Services.	Version 1
20/6/14	Version 1	Amended due to recent archiving of planning guidance documents Revision by Lesley Nesbitt Security Services	Version 2
12/10/2017	Version 2	Inclusion of BREEAM requirements for security points. Added information about Padlocks, trade buttons, window restrictors, bespoke external entrance doors, magnetic locks – failsafe and security, OUSS soft landings requirements included. New CCTV section, links updated. Revision by Lesley Nesbitt Security Services	Version 3
23/04/2018	Version 3	Clarification on door, window and rooflight security standards. (sec: 19.3, 19.5, 19.6, 19.9 and 19.10). Thief resistance electronic door locking security standards added (sec 20.6), Replacement cylinder locks for doors (security standard) added (sec:19.7). Clarification on laminated glazing standards (Sec: 19.3, 19.8, 19.9, 19.11). Updated by Lesley Nesbitt Security Services	Version 4
24/5/18	Version 4	Document reviewed by Isobel Hughes: BREEAM references removed Toilet design references removed. Document renamed: Crime Prevention Design Guide Added Strategic CCTV and Alarm monitoring & technical information inserted (Sec 23 & Sec 24) author Mark Round New security standard - Thief resistant electronic door locking devices (Sec 18.6) Updated by Lesley Nesbitt, Security Services	Version 5

Contents

Introduction 8
1. Designing against crime 8
1.1 Crime Prevention through Environmental Design (CPTED) 8
1.2 Secured by Design 9
2. National Planning Policy 9
2.2 Oxford Local Plan 2036 9
3. Design and Access Statement - Crime Prevention 10
3.1 Crime and Disorder Act 1998 10
3.2 The Design and Access Statement 10
4. Design and Layout 10
4.1 Public and private space 10
4.2 Location and adjoining land use 10
4.3 Configuration of buildings 10
4.4 Outdoor amenity spaces 11
5. Roads and footpaths 11
5.1 Through-routes 11
5.2 Vehicle, pedestrian and cycle routes 11
5.3 Footpaths and cycle routes 11
5.4 Planting next to pedestrian/cycle routes 12
5.5 Lighting of segregated pedestrian/cycle routes 12
6. Perimeter 12
6.1 Creating a secure site 13
6.2 Boundary types 13
6.3 Fencing 13
6.4 Gates 14
6.5 Defensive hedging 14
6.6 Signage and building identification 14
7. Vehicle Parking and Access 14
7.1 Natural surveillance 15
7.2 Secure delivery and collection areas 15
7.3 Multi-storey vehicle parking facilities 15
7.4 Surface parking facilities 16
7.5 Underground car parking facilities 16
7.6 Motorcycle parking 17
7.7 Bicycle parking 17
8. External lighting 18

8.1 Effective lighting 18
8.2 Bollard lighting 18
8.3 Feature lighting 19
8.4 Motion activated lighting 19
8.5 External illumination for buildings 19
9. External security issues 19
9.1 Landscaping 19
9.2 External furniture and litterbins 20
9.3 Natural surveillance and recessed doorways 20
9.4 Temporary buildings 20
9.5 Wind turbines and photovoltaic installations 21
9.6 Heating, Ventilation and Air conditioning (HVAC) 21
10. Internal and external storage facilities 21
10.1 Internal storage facilities: 21
10.2 External storage facilities: 21
11. Utility services 21
11.1 Telecommunications access covers, ducting and utility meters 21
11.2 Utility meters 22
12. Building shell 22
12.1 Windowless building elevations 22
12.2 Night purging and automatic opening window systems 22
12.3 Walls – facades, apertures and graffiti 23
12.4 Roof design, access and aids to climbing 23
13. Internal layout issues 23
13.1 Main entrance 23
13.2 Additional entrances 24
13.3 Reception area and visitor control 24
13.4 Reception good design principles 24
13.5 Internal doorsets 25
13.6 Internal lighting 25
14. Physical Security 25
15. Perimeter – high security 25
15.1 Security Fencing 25
15.2 Security Gates 26
15.3 Security bollards 26
15.4 Padlock Standards 27
16. Closed Circuit Television (CCTV) 27
16.1 External CCTV design 28
16.2 Standalone CCTV systems 28

16.3 Operational Requirement 28
16.4 Strategic CCTV - University Security Services 28
CCTV - Technical information see Section 24 of this document 28
16.5 Department options: Estates CCTV network 28
16.6 The University Security Policy 29
16.7 Data Protection 29
16.8 Camera Surveillance Commissioner (CSC) Code of Practise 29
17. Building envelope 29
17.1 Wall construction 29
17.2 Glazed curtain walling and window walls 29
17.3 Roller shutters and grilles 30
17.4 Roof construction 30
17.5 Roof lights and sun tubes 30
17.6 External door apertures 31
17.7 Lock security standards for doors and gates 32
17.8 Glazing within doorsets and secure vision panels 32
17.9 Window apertures 33
17.10 Secondary glazing 33
17.11 Glazing (laminated glass) 33
18. Access Control 34
18.1Electronic access control 34
18.2 Keyless buildings 34
18.2Magnetic locks and fire alarm activation 35
18.4 Entrance barriers 35
18.5 Trade Buttons 36
18.6 Thief resistant electronic door locking devices 36
19. Mail and parcel delivery 36
20. Internal security considerations 37
20.1 Intruder Detection System (IDS) 37
20.2 Security fogging devices 38
20.3 Public address systems 38
20.4 Physical security standards for vulnerable rooms. 38
20.5 Internal doorsets 39
20.6 Student lockers 39
21. Soft Landings – University Security Services 39
22. Security standards 39
23. Strategic CCTV – Technical Information – Author Mark Round Estates IT Manager 40
Overview 40
Hardware and Software 41

Network Connectivity 41
Responsibilities 41
Design Considerations 41
Variation 41
Costs 41
Contacts 41
Further information 42
24. Alarm Monitoring – Technical Information – Author Mark Round Estates IT Manager 42
Overview 42
Hardware and Software 42
Network Connectivity 42
Responsibilities 42
Design Authority 43
Design Considerations 43
Variation 43
Costs 43
Contacts 43
25 The Checklist 44
Design and Layout 44
Roads and paths 44
Perimeter 44
Vehicle Parking – Cars, bicycles and motorbikes 44
External Lighting 45
External security issues 45
Internal and external storage facilities 46
Utility Services 46
Building Shell 46
Internal layout 46
Physical Security 46
Closed Circuit Television (CCTV) 47
Building envelope - security 47
Access control 48
Mail delivery 48
Internal security considerations 48
Soft Landings – University Security Services 49

Introduction

The University of Oxford is committed to providing safe and sustainable developments where crime and anti-social behaviour, and fear of crime and anti-social behaviour, does not undermine the quality life for staff, students and visitors.

The main objective for including Crime Prevention principals in the design of buildings and their environments is to deter criminal activity and anti-social behaviour by creating developments where opportunities to commit crime are designed out.

Oxford University Security Services (OUSS) have specially trained staff, known as Crime Prevention Design Advisors (CPDA), who will advise, support and guide Estates Services Capital Projects Teams to ensure that Crime Prevention is given due consideration during the development design process from 'Strategic Definition' stage (RIBA 0) to 'In Use' stage (RIBA 7).

The Head of Security Services prepares a regular Strategic Assessment document that details the threats, risks and vulnerabilities that may impact on the University. The identified threats, and vulnerabilities include Crime, Protest and Occupation, Cybercrime, Domestic Extremism, Terrorism and Major Incident Response but of course may change as the current intelligence picture develops over time.

The CPDA will not only consider the Strategic Assessment but will also consider local risks, threats and vulnerabilities that may impact on the proposed Capital Project and provide tailored crime prevention advice, support and guidance referencing the principles of Crime Prevention through Environmental Design (CPTED),Secured by Design (SBD) and Park Mark Safer Parking scheme.

This philosophy document is a **'guide'** to Project Managers, Architects, Project Sponsor Groups', Developers and Consultants and aims to establish good principles for designing against crime. The document addresses the design and layout of a development and physical and electronic security measures.

Within this document is an easy to follow checklist to ensure that all aspects of design and security have been taken into consideration. This document provides guidance on the design and layout of a development and minimum physical security standards which together:

- Create safer and more secure environments.
- Increases the detection of criminal and anti-social behaviour.
- Makes crime more difficult to commit.

All building projects including academic buildings, high risk buildings, post graduate accommodation, refurbishments, extensions and issues concerning designing for Counter Terrorism, should be referred to University Security Services – Crime Prevention Design Advisor.

1. Designing against crime

1.1 Crime Prevention through Environmental Design (CPTED)

The Principles of CPTED are based on the theory that the environment can provide opportunities for crime to occur, therefore changes in the environment can prevent and reduce crime. The behaviour of an offender can be influenced by the design of the environment and this will impact on their rational choice thought processes i.e. '*Will I be seen; If I am seen, will anyone notice me; If I am noticed, will anyone do anything about it?'*

The key strategies of CPTED include natural territoriality, natural surveillance and natural access control:

Natural Territoriality (or defensible space): *Is about people feeling a sense of ownership over a public or semi-public space; well defined space makes the identification of strangers much easier.*

Natural Surveillance: *Increases the chances of someone noticing a potential offender and will deter criminals who don't want to be seen.*

Natural access control: *Is concerned with the locations of entrances, lighting and fencing etc. that can discourage crime.*

1.2 Secured by Design

Secured by Design (SbD) is a Police Security initiative designed to encourage the building industry to adopt prevention measures in the design of developments to assist in reducing the opportunity for crime and reducing the fear of crime by creating safer and more secure environments. Crime and anti-social behaviour are more likely to occur if the following seven attributes of sustainable communities are not incorporated; Clarity in defining the use of space can help to achieve a feeling of wellbeing and limit opportunities for crime.

- Access and movement: *places with well-defined and well used routes with spaces and entrances that provide for convenient movement without compromising security*
- Structure: *places that are structured so that different uses do not cause conflict*
- Surveillance: *places where all publicly accessible spaces are overlooked*
- Ownership: *places that promote a sense of ownership, respect, territorial responsibility and community*
- Physical protection: *places that include necessary, well-designed security features*
- Activity: *places where the level of human activity is appropriate to the location and creates a reduced risk of crime and a sense of safety at all times*
- Management and maintenance: *places that are designed with management and maintenance in mind, to discourage crime in the present and the future, encouraging businesses and legitimate business users to feel a sense of ownership and responsibility for their surroundings can make an important contribution to community safety and crime prevention.*

2. National Planning Policy

The NPPF makes particular reference to *'creating safe accessible environments where crime and disorder, and the fear of crime do not undermine quality of life and community cohesion.'* Sec7 - Requiring Good Design (para: 58); Sec8 - Promoting Healthy Communities (para: 69)

2.2 Oxford Local Plan 2036

Currently under consultation

https://www.oxford.gov.uk/info/20067/planning_policy/743/the_local_plan

3. Design and Access Statement - Crime Prevention

3.1 Crime and Disorder Act 1998

Section 17 (as amended by Schedule 9 of the Police and Justice Act 2006) states: *'Without prejudice to any other obligation imposed on it, it shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent, crime and disorder in its area.'* This obligation extends to local authority planning officers

3.2 The Design and Access Statement

The Design and Access statement that accompanies outline, full or reserved matters planning applications provides an opportunity for the applicant to demonstrate how the development has taken crime prevention into consideration in its design and layout and informs the planning officer that steps have been taken to reduce crime and disorder and the fear of crime and disorder within the proposed development.

The Crime Prevention Section in the Design and Access Statement should address the 7 attributes for creating safe and sustainable paces listed at section 1.2. The CPDA can offer advice, support and guide the Capital Project Team when writing the Crime Prevention section in the Design and Access Statement.

4. Design and Layout

This section looks at the design and issues including defining private and public space, location and adjoining land use, the configuration of buildings and outdoor amenity space.

4.1 Public and private space

Creating an easily legible sense of place where staffs, students and visitors are able to go about their daily routine and business without undue fear crime is a key element to creating safe academic environments. This can be facilitated by clarity in where public space ends and where communal, semi-private or private space begins. Crime and anti-social behaviour are more likely to occur where it is unclear whether space is public or private. Uncertainty of ownership can reduce inherent caring responsibility for space and increase the likelihood of crime and anti-social behaviour going unchallenged.

4.2 Location and adjoining land use

Security requirements may be influenced by the location of new or existing residential or academic buildings, both in the immediate vicinity and in the surrounding area, the hours of operation, the type of learning or research facilities, the numbers of staff and students working on site and number of visitors.

In planning new academic or research areas or when re-developing such areas, sustainable design principles should be utilised, including the relationship of the proposed development with other facilities in the local built and landscaped environment. Security may be significantly improved when the new buildings benefit from natural surveillance from existing occupied buildings. Such measures are intended to create conditions in which potential offenders feel vulnerable to detection. However, reliance on natural surveillance alone is not a guarantee of lower crime risk. Natural surveillance has to work in tandem with defensible space and the presence of persons who can act as potential deterrents or witnesses.

4.3 Configuration of buildings

It is important to consider the crime risks, threats and vulnerabilities that a large number of academic buildings might inadvertently create, such as paths behind buildings and isolated areas set aside for car and cycle parking. Legitimate activity on academic sites can be at a low level at weekends and at night and this inactivity can attract criminals. The configuration of buildings to maximise natural surveillance and create defensible space is therefore of great importance, as careful layout can help resolve many of the crime problems associated with these developments. In appreciation of the fact that site constraints and other matters such as solar heating may ultimately dictate the location and orientation of buildings the CPDA will work closely with the designers to ensure the best outcome.

4.4 Outdoor amenity spaces

The location of outdoor seating and socialising areas provided for the use of staff, students and visitors must be as much planned as the buildings. Such amenity space should be within view of overlooking buildings that are likely to be occupied. Recreational spaces may encourage trespass outside of normal business hours and may require additional security measures.

5. Roads and footpaths

This section reviews through routes for vehicles, pedestrians and cyclists, planting and lighting of footpaths and cycle routes.

5.1 Through-routes

Where through-routes may be included within layout of an academic development the designer should ensure that the security of the development is not compromised by excessive permeability, such as allowing the criminal legitimate access to the rear or side boundaries of buildings or providing too many escape routes by designing in unnecessary segregated footpaths. The provision of surveillance provided by overlooking buildings would be beneficial and controlling and limiting permeability and the creation of defensible space can reduce opportunity for crime to happen.

5.2 Vehicle, pedestrian and cycle routes

Vehicular, pedestrian and cycle routes should be visually open, direct, and well used and should not undermine the defensible space of the academic site or development. Design features can help to identify the acceptable routes through a development, thereby encouraging their greater use and in doing so enhance the feeling of safety. Where it is necessary to limit access features such as rumble strips, change of road surface (by colour or texture), pillars or narrowing of the carriageway may be used. This helps to define the defensible space, psychologically giving the impression that the area beyond is private.

5.3 Footpaths and cycle routes

The pedestrian/cycle paths should be as much 'designed' as the buildings. It is a good design principle that routes for pedestrians and cyclists run alongside one another and not be segregated and networks of separate pedestrian/cycle routes to unsupervised areas should be avoided. All planned routes should be needed and follow desire lines, thus generating adequate footfall and they should be well overlooked and integrated. Underused alleyways, shortcuts and a large number of minor access points can create hiding areas and anonymity for offenders.

If segregated pedestrian/cycle routes are unavoidable, designers should consider that such routes can facilitate crime. Where necessary and where space permits, segregated cycle and pedestrian paths should be at least 3 metres wide (to allow people to pass without infringing each other's personal space), with at least a two-metre verge on either side. These routes must be straight, wide, well lit, avoid potential hiding places and be overlooked by surrounding buildings and activities. It is important that there is good visibility along the route of the pathway.

Ideally public footpaths should not run to the rear of academic buildings, rear yards or neighbouring buildings as these designs generate crime. Private footpaths that serve as emergency exit routes at the rear of academic buildings should be secured with gates and locking systems that restrict access but still facilitate emergency egress, without hindrance. **Seek further advice from the University Fire Officer on suitable locking mechanisms for emergency egress.**

Keeping pedestrians, cycles and vehicles at the same level avoids creating intimidating spaces such as subways, footbridges and underpasses. If a subway is essential it should be as wide and as short as possible with a clear line of sight to the exit. Chamfering the access points can help reduce areas of concealment.

5.4 Planting next to pedestrian/cycle routes

Planting next to a pedestrian/cycle route should begin at the outer edge of the verge, starting with low growing plants with taller shrubs and trees to the rear. Planting immediately abutting the path should be avoided as the plants could have a tendency to grow over the path creating pinch points, places of concealment.

Where pedestrian/cycle routes run next to buildings or roads the path should be open to view. This does not prevent planting, but will influence the choice of species and the density of planting. Pedestrian/cycle routes should not run immediately next to doors and windows, therefore buffer zones should be created to separate a path from a building elevation, defensive planting should be considered.

Careful selection of plant species is critical to promote natural surveillance and to avoid unnecessary maintenance. **Seek further advice from the University Parks Superintendent on suitable plant types.**

5.5 Lighting of segregated pedestrian/cycle routes

The need for lighting will be determined by local circumstances. In a city environment the lighting of a pedestrian/cycle route is generally only effective in reducing crime levels (or preventing them from rising) if it is matched with a high degree of natural surveillance from surrounding buildings where reaction to an identified incident can be expected i.e. a witness calls the police, or the route is well used. The lighting of an underused route may give the user a false sense of security, in these circumstances it might make more sense to close the path at night rather than light it.

Pedestrian/cycle routes that are to include lighting should be lit to appropriate levels as defined in BS 5489. It is important that the landscape architect and lighting engineer co-ordinate their plans. This will help avoid problems such as conflict between lighting and tree canopies, reducing dark shadowed areas. **Seek further advice from the Electrical Department at Estates Services.**

6. Perimeter

This section reviews perimeter treatments, boundary types, fencing, gates, defensive hedging, signage and building identification.

6.1 Creating a secure site

It is acknowledged that the vast majority of existing academic and research building developments are served by road, cycle and pedestrian networks that are deliberately designed to provide accessibility to the public. Therefore clearly defined boundaries using fences, walls, hedges and other demarcation treatments will need to be considered.

Ideally, no part of an academic or research building should immediately abut a public footpath, road or other public area. This is to prevent a vehicle borne attack to penetrate a wall, door or window or to prevent parking of high sided vehicles close enough to the building to allow climbing to upper, perhaps less secure windows or flat roofs.

In open planned developments a defensible area can be created between the units and the public routes by the introduction of car or cycle parking and measures such as high kerbs, dwarf walls and hard and soft landscaping. Access for pedestrians or vehicles along the side of a building should be controlled through the use of fencing and or gates and additional physical barriers, such as 'anti-ram' bollards, roller doors and shutters may also be required to protect vulnerable elevations.

Hard and soft landscaping should not obstruct visibility of doors, windows or any other access points. Casual approaches to windows can be deterred through the creation of uneven hard surfaces such as cobles or angled brick sets set in concrete. Particular care should be taken when specifying the type of gravel or loose surface treatment in developments so as not to provide missiles which will create criminal damage opportunities.

6.2 Boundary types

Boundaries fall into three main categories:

Psychological: *Those that are intended to psychologically define ownership of space and distinguish between private and public land using features such as rumble strips, change of road surface (by colour or texture), road markings, and landscaping*

Controlling: *Normally a low fence, knee high railings, a wall, hedge or other boundary treatment intended to help staff manage a site by physically restricting casual intrusion onto the site and channelling visitors to a formal entrance point in the perimeter. These types of boundaries are generally not high enough or sufficiently resistant to intrusion to be classified as a secure boundary.*

Securing: *A fence, wall, hedge or other boundary treatment intended to physically prevent climbing or penetration into restricted parts of the site. It is important that there are no structures close to the fence that will aid climbing such as trees, lamp columns, waste bins and storage units.*

6.3 Fencing

(High security fencing see section 15.1). The demarcation between public space and University development is important, and in some cases there may be a need for fencing that offers greater security in order to protect a particular risk. It is therefore important that the boundary treatment is discussed in detail with the CPDA at the earliest possible opportunity.

The five main reasons for providing a perimeter boundary fence are to:

- Mark a boundary to make obvious what is private and what is public property.
- Provide safety for employers and employees.

- Prevent casual intrusion by trespassers.
- Prevent intrusion onto the site by criminals.
- Reduce the wholesale removal of property from the site by thieves.

The height of the fence will be determined by local circumstances, crime risk and the system chosen. In most circumstances heights between 1.2m and 2.4m will be sufficient.

Public through-routes immediately outside the boundary fencing can affect security. If the route already exists and cannot be re-routed, the use of defensive planting in addition to fencing should be considered. However, care should be taken not to block natural surveillance from the through-route into the development and vice versa.

A party or shared boundary should not compromise security and maintenance. It may be advisable to erect a separate fence inside the party boundary, ensuring access for maintenance of both existing and new structures. This arrangement may create a new path around the boundary and measures may be required to obstruct this path at vulnerable points.

6.4 Gates

(High security gates see section 15.2) - The design, height and construction of any gates within a perimeter fencing system should match that of the adjoining fence and not compromise the overall security of the boundary. Gates should be hung so that they are not easily lifted from their hinges and the gap at the bottom of the gate should be narrow so that no one can slip underneath it. The style of the gate should not provide footholds, creating an informal climbing point, which would allow it to be used as a ladder to gain easy access.

6.5 Defensive hedging

In some locations it may be a planning requirement to use or retain a defensive hedge, such as Hawthorn, as a means to protect a site perimeter or to further bolster the security of an existing or proposed fence.

Seek advice from the University Parks Superintendent for further advice on plant species.

6.6 Signage and building identification

Building locations, reception areas, cycle and car parking areas should be clearly signposted from the entrances onto the site. Clear name plates or numbers of individual buildings and departments are essential to assist staff, students, visitors, mail and parcel deliveries and emergency services to locate the right building. Likewise, signs that identify areas that are not open to public access can act as a reminder that unauthorised persons should be challenged.

Where there is an accumulation of academic buildings in one area site maps are a useful way to identify road names and department locations. They should be clearly visible and where necessary protected a clear cleanable cover.

7. Vehicle Parking and Access

This section reviews emergency vehicle parking, secure delivery areas, multi-storey parking, surface parking, underground parking and long and short term cycle parking.

7.1 Natural surveillance

The routes from the site entrance to the reception, to the car parks and delivery points should be clearly defined and benefit from natural surveillance from overlooking buildings especially from the reception areas and other occupied rooms.

Allocated staff and student cycle/car parking should be provided in view of occupied rooms and where possible identified visitor parking should be similarly located. In areas of high crime or where there are special security considerations, secure the parking facility with appropriate fencing or an automatic access-controlled gate or shutter.

7.2 Secure delivery and collection areas

It is good practice to ensure that academic and research buildings are designed to allow secure deliveries and collections of materials and goods. In some cases this may dictate the height of the delivery door and overall dimensions of the delivery bay. Dependant on the risk, threats and vulnerabilities it may be necessary to monitor the loading bay with CCTV.

7.3 Multi-storey vehicle parking facilities

Where a multi-storey parking facility is being designed the following best practise features should be included:

- The car park boundary should be clearly defined and prevent the unauthorised removal of vehicles from the ground floor level.
- Pedestrian access gaps in the perimeter should be controlled in a way to reduce opportunity for casual intrusion by a potential offender to commit crime.
- The gaps between the lower car park levels should be treated in a way to reduce opportunity for climbing and for casual intrusion to facilitate crime. The insertion of a physical barrier such as mesh grills or similar will reduce this opportunity to commit crime.
- It should also be noted that it is not uncommon for people to go to the top of multi storey car parks and jump off, it is therefore advisable to reduce the opportunity for this to occur by increasing the height of the perimeter edge at high levels and treat them in such a way to reduce opportunity for climbing.
- CCTV should be considered to monitor the parking facility and in any event the cabling should be installed for future CCTV installation.
- The stairwells should have open balustrades to aid surveillance between floor levels and where landings or stairwells are external facing they should be designed to maximise natural light into the areas.
- The lighting in the car park should be fit and sufficient for purpose and constantly illuminated during the hours of darkness. White light is preferred.
- Lifts should be fitted with a vision panel in the doors to aid visibility out onto the landing before the doors open, they should be fitted with vandal resistant buttons/panel and there should be an alarm button. An audio link to facilitate communication to outside help is beneficial.
- Signage should be clear, easily cleaned and convey messages to control, warn or instruct the car park users, they may be wall or post mounted. Signs should clearly show where entrances, exits, payment machines, and lifts are and clearly indicate the parking level numbers.
- Parking bays, direction arrows and other floor painted signs should give clear direction and be clearly visible and well maintained.

- Where possible, pedestrian routes through the car park should be segregated and clearly marked.
- All walls and ceilings should be painted with a light reflective colour and be graffiti resistance by using anti-graffiti coatings, rough uneven surfaces or highly patterned surfaces.
- Access ramps should be rough or uneven surfaces to reduce misuse of them by skateboarders.
- Supporting pillars should be carefully designed to promote maximum opportunity for surveillance across the car parking levels, circular pillars are preferred.
- The overall design of the car park should avoid creating dark or hidden areas.
- Where a car park design incorporates an area for delivery vehicles this area should be accessed by a separate entrance to the car park and the delivery area would benefit from being secured by using shutters or grills.
- The use of height restrictors at the car park entrance would control the type of vehicle entering the car park.

7.4 Surface parking facilities

Where surface vehicle parking areas included they should be designed to incorporate the best practise features listed below:

- A suitable boundary treatment for the car park needs to be considered, hedging and or railings are often suitable as they control access into the car parking area but still allow for natural surveillance.
- Where trees and hedges are being included in the design to soften the impact of the vehicles the tree canopies should be at least 2 metres from the ground level and hedges should not be more than 500mm in height this provides for good surveillance opportunities across the parking area.
- Uniformity of lighting is crucial in creating a safer car parking environment, lighting should not be designed to create dark shadowed areas. Bollard lighting should be avoided in surface car parks and white light is preferred.
- CCTV should be considered to monitor the parking area and in any event the cables for the later CCTV installation should be incorporated in the development.
- Large parking areas benefit from having a one way traffic flow system in operation and good clear signage indicating the exit route is essential to avoid conflict.
- Where possible, pedestrian routes passing through the vehicle parking area should be segregated and clearly marked.
- Parking bays should be clearly marked and any parking restrictions should be displayed on prominent signs.
- Parking meters should be located in prominent positions and be well illuminated during the hours of darkness.

7.5 Underground car parking facilities

Where a development incorporates an element of underground car parking then the developer should note that the following best practise measures for creating safe parking areas:

- Every effort should be made to prevent unauthorised access into the car park, therefore, an access control system must be applied to all pedestrian and vehicular entrances.

- Inward opening automatic gates or roller grilles/shutters should be located at the building line or at the top of ramps to avoid the creation of a recess. They should be capable of being operated remotely by the driver whilst sitting within the vehicle, the operation speed of the gates or shutters should be fast enough to avoid tailgating by other vehicles. All motorized grilles or shutters must be installed with appropriate safety detection systems to avoid personal injury or damage to vehicles.
- Automatic roller shutters should be certificated to LPS 1175.
- Lighting should be at the levels recommended by BS 5489-1:2013.
- The lighting system may be a part time system based upon a pre-determined period after the main vehicle or pedestrian doorset has been opened or alternatively a system utilising passive infra-red detectors, or similar, to activate the lighting.
- Walls and ceilings must have light colour finishes to maximise the effectiveness of the lighting, this will reduce the number of luminaries required to achieve an acceptable light level.
- Any internal door that allows access to the main building or office floors above must have an access control system and meet the physical requirements as advised by the CPDA. **Refer to the University Fire Officer if the door is a means of fire escape.**
- In larger developments Closed Circuit Television (CCTV) may be required in which case the CCTV must be capable of being recorded and monitored.

7.6 Motorcycle parking

Covered and secure motorcycle, moped and scooter parking should be made available and such parking provision should benefit from surveillance from an occupied building, be provided with 'Sold Secure' silver or gold standard ground anchors and be lit after dark when in use.

It is recommended that two wheeled motor vehicle parking areas are cement finished as opposed to tarmac finished as this reduces the opportunity for the motorcycles to sink into the ground.

7.7 Bicycle parking

Long and short term parking - Ventilated, bicycle stores within the main building must either have no windows or windows with security grilles and be fitted with a secure doorset that meets the standard required by the CPDA. The locking system must be operable from the inner face by use of a thumb turn to ensure that persons are not accidently locked in by another user. The lighting in such a building must be automatically activated. The store should contain cycle stands where it is possible for the cycle to be securely locked in two places.

Where it is not possible to make long term cycle storage available within the main building then an external covered and secure structure should be considered and include the following features:

- It should be within sight of occupied buildings. It should be fitted with cycle stands to allow the cycle frame to be locked in two places.
- It should be illuminated during the hours of darkness.
- Secured entrance doors should be fitted with a robust closure so that it automatically closes as people pass through it reducing the opportunity for the door to be left open accidently leaving the parked cycles vulnerable to theft.
- Care should be taken that the securable roofed structure does not provide easy access onto nearby roofs to reach high windows or other flat roofs.

- The secured cycle storage area should not be a solid construction as this will minimise natural surveillance opportunities, a transparent storage unit is preferable.
- External containers specifically designed for the secure storage of 2 and 3 bicycles and certified to LPS 1175 SR1 are available and may be suitable for long term storage.

Short term visitor cycle parking provision is probably the most vulnerable to crime and should include the following features:

- It should be located within clear view of occupied buildings.
- The design of the cycle stand should allow for the cycle frame to be locked securely in two places. (Sheffield hoop design)
- The cycle parking area should be lit during the hours of darkness.
- Where appropriate CCTV should be considered.

8. External lighting

This section includes effective lighting, bollard lighting, feature lighting, motion activated lighting and the external illumination of buildings.

The lighting strategy must be discussed with the CPDA and the Estates Services Lighting Engineer and care should be taken that landscaping, tree planting, CCTV and lighting schemes do not conflict with each other.

NB: If the proposed lighting strategy is within a conservation area or includes a Scheduled Ancient Monument or Listed buildings the external lighting strategy will need to be referred to the Conservation and Buildings department at Estates Services.

8.1 Effective lighting

To be effective, lighting should ensure a realistic chance that there will be witnesses to an intrusion. It should also make intruders feel vulnerable to detection and an increased risk of being challenged. Perversely, installing lighting which cannot achieve this effect, such as the lighting of an elevation that cannot be observed by potential witnesses or CCTV, may actually assist an intruder.

The evenness of light distribution or uniformity of lighting (Uo), is almost always more important than the levels of illumination being achieved by the system. Guidance for lighting levels are determined by latest edition of BS 5489. Avoid creating pools of light and dark shadowed areas because crime levels, and in particular fear of crime levels, can be affected by inappropriate lighting levels.

Best practise suggests that the Colour Rendering qualities of lamps used on a development should achieve a minimum of at least 60Ra (60%) on the Colour Rendering Index. The ‘whiter’ the light the better the colour rendition qualities. Properly controlled white light will illuminate an area to higher satisfaction levels for people whilst actually delivering less light than would be required for similar levels of satisfaction if non-white light sources were used.

8.2 Bollard lighting

Bollard lighting is very useful for ‘way finding’ but used alone will not produce enough light to create an environment that feels safe. This type of lighting creates pools of light and areas of darkness, it can distort facial features, increasing the fear of crime as it is not possible to distinguish between friend or foe. If cars park up against the bollard light the effectiveness of the light is reduced significantly and bollard lights are often damaged and left lying on the ground.

8.3 Feature lighting

Feature lighting is similar to bollard lighting and alone it will not produce enough light spills to create an environment that feels safe. Dependent upon the location of the feature lighting it may be necessary to include additional lighting to achieve appropriate lighting levels.

8.4 Motion activated lighting

Motion activated security lighting is effective in areas that do not benefit from natural surveillance as a light activation indicates that there is movement in the area, however, this type of lighting should not be used in an area frequently used by staff, students or visitors as the sudden change in light levels will cause partial blindness and it will take considerable time for eyes to adjust to the sudden bright light.

8.5 External illumination for buildings

External illumination for buildings is recommended for routes to the main entrance, other external doors, car and cycle parking areas and observable building elevations. When a building is closed it may be appropriate to operate this lighting via movement detection devices. In this case consideration must be given to using the most efficient detectors to avoid sudden unnecessary glare where it would take considerable time for the human eye to adjust to sudden variations in lighting levels.

9. External security issues

This section reviews landscaping, external furniture and litter bins, natural surveillance and recessed doors, temporary buildings, wind turbines and photovoltaic installations and heating, ventilation and air conditioning (HVAC)

9.1 Landscaping

The CPDA should review the proposed Landscape Strategy for the development. The landscape strategy should be developed at an early stage of the design process and considered in tandem with the CCTV and lighting strategies to avoid and reduce future conflict between these three elements.

The selected use of plants such as spiny or thorny shrubs can help prevent graffiti, casual approaches to the external face of the building, loitering and can create or enhance perimeter security. Defensive planting is not just about prickly shrubs. It is about selecting the right type of plant for the right aspect and environment. For example, open branched and columnar trees can be used in a landscape scheme where natural and formal surveillance is required. Climbing plants can be used to cover walls that may be used as canvases for graffiti and carefully selected trees and shrubs can be used to “green up” the most hostile of environments providing both horizontal and vertical interest without adding to crime risks. **Seek further advice from the University Parks Superintendent on defensive plant types.**

Planting should not impede the opportunity for natural surveillance and must avoid the creation of potential hiding places. In order to provide a window of surveillance opportunity shrubs and bushes should be maintained at a height of no more than one meter and tree canopies should be more than 2 metres from the ground. Plant growth below 500mm is ideal in areas designated for car and cycle parking as it exposes potential offenders and deters vehicle interference and theft.

Species selection of trees and shrubs should take account of their future maintenance, as poor maintenance can impact on site security. **It is recommended that the University Parks Superintendent and appointed Landscape Architect are consulted about these matters.**

9.2 External furniture and litterbins

External furniture such as benches and planters should be of robust, vandal and graffiti resistant. Furniture should be fixed into the ground in order to prevent its theft and reduce the possibility of it being used for climbing onto roofs and over boundary fencing or as a tool to break through the shell of the building.

The design of benches should be carefully considered, the use of arm rests and shaped seats can reduce the opportunity for them to be abused by skateboarders and rough sleepers.

Litterbins can also be used to assist climbing and its contents used to start fires. It is preferable that the litterbins are of a type that can be locked onto a fixed base and that they are located away from the buildings. Under no circumstances must litterbins be wall mounted beneath windows or on walls covered in combustible material.

Dependent upon the risks, threats and vulnerabilities of the area it may be advisable to install litter bins that use clear plastic bags so that the items inside can be easily seen.

9.3 Natural surveillance and recessed doorways

It is important to avoid creating areas and building features (such as recesses) that cannot be overlooked from another occupied building or room. Recessed doorways can obstruct surveillance and also collect windblown litter that can be used to start fires. Designing in unobservable recesses and then providing CCTV surveillance of the recess is not a sustainable solution.

Where a recessed doorway is unavoidable because of site constraints, a security rated door with emergency exit hardware and in-built secure vision panel may be recommended.

9.4 Temporary buildings

Temporary buildings, such as portable buildings, are difficult to secure due to their construction and the fact they are outside the secure envelope of the permanent building structures. The voids under many of these buildings must be designed to prevent the concealment of items and litter collecting underneath, which may be used to start a fire.

Temporary buildings should not be used for the storage of high value equipment and they should be included within the main building's intruder alarm system, and care should be taken to protect the cables supplying power to the temporary building alarm system.

If possible additional temporary buildings should be linked to each other to form one larger continuous building, thus avoiding the creation of blind spots in between the buildings. The use of non-security rated temporary buildings should be discontinued as soon as possible.

Wherever possible temporary and portable buildings should be constructed of non-combustible materials.

The location of temporary buildings must be discussed with the University Fire Officer, to ensure that the spread of fire to other buildings is minimised and that the fire service's access is not restricted.

9.5 Wind turbines and photovoltaic installations

Consideration must be given to protecting wind turbines, photovoltaic installations (PVs) and biomass boilers from vandalism through the use of access control, such as suited keys, appropriate fencing and the removal of any climbing facility that may aid access.

PV panels are susceptible to criminal damage from thrown missiles. Therefore PVs should be located on roofs that are difficult to access, other than by legitimate means, and should be secured onto the roof with theft resistant fastenings. Care should be taken when the design of the landscape includes the use of loose pebbles for obvious reasons.

9.6 Heating, Ventilation and Air conditioning (HVAC)

Where identified risks, threats and vulnerabilities dictate air takes for the HVAC system should be located in a secure area and ideally at level 2 or above of the building. It should have the capability of rapid shut-off.

Seek further advice from the Mechanical and Electrical Department at the University Estates Services for HVAC systems.

10. Internal and external storage facilities

This section reviews internal and external storage facilities for hazardous and non-hazardous items and waste.

10.1 Internal storage facilities:

Cleaners cupboards/rooms – the cleaners cupboard should have the capability of being locked, this will avoid unnecessary incidents of petty theft.

Hazardous waste storage – Consult with the Hazardous Waste Technical Officer at the University Safety Office.

10.2 External storage facilities:

Non-hazardous waste storage – Waste containers especially those with wheels, can be easily moved and used for climbing and the contents can be used to start fires and heavy items can be placed inside them and transported away. Consideration should be given to using waste containers with lockable lids and where appropriate they should be anchored to the ground or stored inside a secure, externally accessed store, in the main building or in an external secured, roofed compound. The waste bins should not be located close to nearby hazards.

Flammable Liquid Storage – Consult with the Hazardous Waste Technical Officer at the University Safety Office

Hazardous Waste Storage – Consult with the Hazardous Waste Technical Officer at the University Safety Office.

11. Utility services

This section reviews securing utility covers and the location and access to utility meters.

11.1 Telecommunications access covers, ducting and utility meters

Telecommunication lines and cables should enter buildings below ground and be protected by secure access covers and be positioned in highly visible locations. This will help to delay or prevent the occurrence of burglaries where the perpetrators cut the CCTV or alarm signalling wiring prior to undertaking the offence.

The ultimate security of the buildings may be reliant upon the intruder or fire alarm's ability to signal to an alarm receiving centre via a secure telephone line. It is therefore important to provide sufficient secure ducting into the site with an appropriate number of secure access covers.

11.2 Utility meters

Utility meters benefit from being located in a secure building, such as a plant room, and where possible should allow for meter reading without having to enter the main building. Alternatively, instructions should be given to utility providers to carry out their readings during hours of occupancy or by prior appointment, so that access can be arranged without increasing security risk.

Utility access covers, protecting access to drains, sewers, electricity cables and other services, should be secured to prevent access and damage by unauthorised persons.

12. Building shell

This section reviews the design of the building shell which is crucial in reducing opportunity for crime to occur and includes windowless elevations, night purging, automatic opening windows, walls, apertures and facades, roof design and climbing aids.

12.1 Windowless building elevations

A feature of some academic and research buildings are long elevations that have no windows, and windowless emergency exit doors which are often recessed. This design can present opportunities for crimes such as graffiti, burglary and arson and also inappropriate loitering.

Where possible unauthorised persons should be kept away from such building elevations, they can be protected in a number of ways:

- Access footpaths can be gated, it will be necessary to provide easy egress if this is a fire escape route. For further advice refer to the University Fire Officer.
- Create a 1m or greater separation between the footpath/road and the building elevation by using a 1.8m high fence or defensive planting.
- Install a security rated doorset.
- Check the construction of the wall – is it vulnerable to intrusion?
- Anti-graffiti coatings or a suitable wall surface finish capable of being painted will assist with controlling graffiti.
- Consider growing an appropriate non-invasive climbing plant up the wall.
- If appropriate insert a security rated window at ground floor level.

12.2 Night purging and automatic opening window systems

It is essential the night purging strategy, including automatic opening window systems and vents, designed to operate when the building is largely unoccupied, should only be designed to operate from the first floor level and above; this will maintain the security of the ground floor windows whilst allowing windows at above ground level to open or be opened to ventilate the building.

Care must be taken not to compromise the security of the building at above ground floor level if the opening windows are easily accessible.

12.3 Walls – facades, apertures and graffiti

Building facades should minimise the opportunity for hiding and climbing up to windows or onto roofs therefore avoid unnecessary deep ledges, parapets, indentations and protrusions.

The potential for unauthorised entry via the goods lifts, fuel delivery points or ventilation ducts should be considered. Where possible such services should be concealed and/or located in locked compartments. Grilles, air ventilation apertures and shutters should be fitted so that they cannot be removed to permit unauthorised access, additional physical security measures may be necessary.

As graffiti tends to attract further graffiti it is always advisable to remove it as soon as possible. Designers should consider wall finishes that make this task easier to perform, anti-graffiti coatings should be considered.

12.4 Roof design, access and aids to climbing

Designers should take care not to create climbing aids to upper windows and flat roofs via structures such as boundary walls, handrails, deep window sills, drainpipes and external staircases.

Flat roofs, particularly those at a low level, are easily accessed and depending on materials may be more vulnerable to intrusion either by cutting through the deck or forcing open roof lights and other openings.

The building design should prevent easy access to roofs, external rainwater pipes should be either square or rectangular in section, flush fitted against the wall or contained within a wall cavity or covered and bends creating footholds in pipes and horizontal runs should be minimized.

13. Internal layout issues

This section reviews the design of the main entrance, additional entrances, reception areas and visitor control, the location of toilets, internal doorsets and internal lighting.

13.1 Main entrance

Main entrance door(s) should be clearly identifiable to visitors and in clear view of reception staff. Where necessary the entrance door should be electronically access controlled permitting authorised users to enter or for visitors to enter once the doors are released from a reception desk or office. The inclusion of an audio visual intercom unit linked back to the reception will be determined by the buildings layout and the identified threats, risks and vulnerabilities.

It may be appropriate to use an 'airlock' door system whereby two sets of automatic doors are used, the first set of doors opening upon the detection of a visitor and the second set of doors, either opening in the same fashion or controlled from the reception desk. It should be possible to control and lock both opening doors from the reception desk. In some high risk situations the design the airlock door system may mean the external door has to shut too before the internal door can be opened.

During normal opening hours it is common practise for the main entrance door to allow uninterrupted access straight into a reception lobby area and then onward movement through the building is controlled by internal barriers or access control systems on internal doors.

External entrance doors should be fitted with an additional key operated lock to enable a managed lock down of a building in the event of complete power failure or an extraordinary external event that necessitates a 'building lockdown' situation.

13.2 Additional entrances

There may be instances, especially with large buildings, that further entrance doors will be required for the convenient movement of staff, students and visitors. The crime opportunity risks that this arrangement might create will have to be properly managed, and be addressed in the access control strategy. It may be necessary to install internal entrance barrier gates and/or CCTV monitored by reception staff to oversee who is entering the building, and to identify those who may require assistance. (For further information on entrance barriers see also section 19.3)

13.3 Reception area and visitor control

The reception area should create a positive and interesting impression of the University department(s). Colour schemes and textures of wall finishes and furniture should be carefully considered to create a calming environment for waiting visitors. Behind this outward impression lies the main function of the reception area, which is the effective and appropriate management of visitors, which is critical to the buildings security.

Where large numbers of visitors attend the building it is recommended that the reception is staffed or supervised at all times. Access beyond the reception area should be controlled using access controlled doors or barriers.

13.4 Reception good design principles

It is important to minimise the risk of assault on all persons on the premises. It is therefore important to plan for the risk of violent incidents even though the risk may be very small:

- Reception desks should provide positioned to give the receptionist a clear view of the waiting area, the approach to the entrance door
- Have restricted access from the public side
- It may be appropriate to fix reception furniture to the floor or walls
- The desk design should include locking cabinets to store loose stationery items
- Do not plan to position tall display units, large flower displays and sculptures so that they obstruct surveillance opportunity across the reception area
- Reception desks should be high and/or wide enough to afford protection for the receptionist and the design should consider the needs of a wheelchair user.

Seek advice from the University Accessibility Adviser

- Where appropriate an escape route to a place of safety, such as an office located behind the reception area, should be provided. A 'slam to lock' door between the reception desk and the place of safety should include a door viewer or secure vision panel to allow a view of the reception area from the place of safety
- Audible/monitored personal attack alarm (PA) points should be located at the reception desk so that the receptionist can use it to summons assistance if confronted by an aggressive visitor. Consideration should be given to an additional alarm sounder located in nearby offices where other members of staff can be alerted. By arrangement PA activations can be monitored by OUSS

Advice should be sought from the Operations Manager at Security Services about this service and relevant fees.

13.5 Internal doorsets

Some rooms may need to be more secure than others during working hours and an early indication by the client as to the various uses will be helpful to determine whether a security rated doorset will be required for a particular room.

As a general rule all internal doorsets should be fitted with locking furniture so that they can be locked when the room is left unoccupied. This is often achieved by using an electronic access controlled system or physical key locks.

Advice must be sought from the University Safety Office for the specifications of security rated doorsets for containment laboratories and radio-active sources.

13.6 Internal lighting

It is recommended that most internal office lighting is operated by detection devices which will automatically switch lights on and off due to movement activity or the lack of it in each room. Such a system can identify the presence and progress of intruders in the building when it is closed.

If such a system is not being proposed then areas inside the building that may require 'out of hours' lighting include any critical area used for movement that can be seen from the outside, e.g. entrance foyers, corridors, staircases and landings. Two-stage lighting can be used internally to save energy whereby a higher level of lighting is triggered by movement.

If the building is a listed building the internal lighting strategy will need to be referred to the Conservation and Buildings department at Estate Services.

14. Physical Security

It is important for the Project Manager and future building occupiers of the proposed building to liaise with their respective insurers to ensure that the proposed security standards meet with the insurers' requirements.

Security standards - It is important that an effective and realistic level of physical security is incorporated into building construction. The CPDA will justify a requirement for enhanced security standards above the minimum standards, referenced through this document, by assessing the risks, threats and vulnerabilities of the building or development based primarily on the location and anticipated use of the premises to be developed.

15. Perimeter – high security

This section reviews security rated fencing, security rated gates, and security bollards.

15.1 Security Fencing

Some security rated fencing systems can be both costly and aesthetically unpleasing. However, the type of fencing that is required must ultimately be determined by local risks, threats and vulnerabilities. For example, where the perimeter of the site is very large it may be more cost effective to install an inner security fence or create a secured area.

In circumstances where assessed risks, threats and vulnerabilities are identified as 'high' a fence that is resistant to intrusion may be required. The minimum standard for this type of fencing will be a system that is certified to LPS 1175 Security Rating 1 or above or Sold

Secure Gold standard or higher. All entrance gates must be of the same high security standard.

Generally fence heights of 1.2 metres to 1.8 metres are suitable for boundary demarcation and controlling movement only and not for security. The height of security fencing will start at 1.8 metres high and it should be capable of raking or stepping to maintain its height over different ground levels without creating gaps underneath. Pedestrian and other entrance gates should be inward opening and the design should match that of the fence. The locking method for the gate should be discussed and agreed with the CPDA.

The fence design should resist climbing and be capable of incorporating a trellis topping. It is important that there are no structures positioned close to the fence that will aid climbing such as trees, lamp columns, waste bins and storage units.

Surveillance of and over the site from any surrounding streets, footways and occupied buildings can help to deter potential offenders. It is therefore recommended that, where appropriate, security fencing systems are not solid structures to facilitate observation from outside the site. The use of dark coloured coatings on welded mesh type metal fencing systems reduce the reflection of light and make it easier for someone passing by to observe activity through the fencing.

15.2 Security Gates

Gates providing reduced access down the sides of buildings should be tested and certified LPS 1175 SR 1, and be constructed as anti-climb designs.

15.3 Security bollards

Generally used for vehicle mitigation - Before specifying security bollards the risks, threats or vulnerabilities facing the premises must be fully assessed to establish if there is a realistic chance of a vehicular borne attack to enter the premises or penetrate the shell of the building. In the first instance consideration should be given to designing in mitigating measures to reduce the angle and speed of an approaching vehicle. The CPDA will offer advice and guidance in relation to designing for Counter Terrorism and liaise with local Police Counter Terrorism Security Advisor.

Where it is not possible to design in mitigating measures to reduce the speed and angle of approach by a vehicle or the risks, threats and vulnerabilities are high the following details will need to be established:

- The type of vehicle(s) likely to engage in an attack – car or HGV.
- The weight of vehicle(s) – probably up to 7.5 tonnes fully laden.
- The maximum speed – 30 to 50 mph.
- The angle of the attack in degrees from the horizontal line.

It is unlikely that the University CPDA will have access to sufficient information to correctly specify the type of security bollard beyond citing PAS 68 & PAS 69 or IWA 14 and the specification is best left to the manufacturers or suppliers.

Bollards intended to prevent vehicle access should stand at least 1 metre high above ground level and be spaced a maximum distance of 1.2 metres between bollards measured at 600mm above ground level.

15.4 Padlock Standards

A concise guide to the different types of padlocks and the corresponding insurance/security ratings

Security protection	European committee for standardisation (CEN)	British /European Standard BSEN 12320	Sold Secure	Loss Prevention Certification Board LPS 1654
Low Security *Garden gates, single tool boxes, securing furniture etc.*	Grade 1&2			Security Level 1
Medium Security *Sheds, electrical cabinets, small gates low cost cycles etc.*	Grade 3	Grade 3	Bronze	
Security protection	**European committee for standardisation (CEN)**	**British /European Standard BSEN 12320**	**Sold Secure**	**Loss Prevention Certification Board LPS 1654**
High Security *Heavy duty gates, security bollards, containers, storage units, security shutters, expensive cycles etc.*	Grade 4/5	Grade 4/ 5	Silver	Security Level 2/3
Ultra-High Security *Warehouse doors. Containers, security doors, machinery motor bikes, large steel gates etc.*	Grade 5/6	Grade 5/6	Gold	Security level 4+

16. Closed Circuit Television (CCTV)

CCTV is not the single solution to security problems, but the provision and effective use of CCTV fits well within the overall framework of security management and is most effective when it forms part of an overall security plan. It can help reduce the fear of crime, deter vandalism and burglary and assist with the identification of culprits once a crime has been committed.

16.1 External CCTV design

Should be co-ordinated with existing or planned lighting and landscaping designs to ensure that the quality of the CCTV images are not compromised by overgrown foliage or flareback from lighting. CCTV cameras may need protection within a vandal-resistant housing.

16.2 Standalone CCTV systems

It is not uncommon for university departments to install a standalone CCTV system that they monitor and record, these systems may include internal and external cameras. The University CPDA can offer advice, support and guidance when designing standalone CCTV systems.

16.3 Operational Requirement

A CCTV system must have clear objectives, it is good practise to establish a policy for its use and operation before it is installed. An 'Operational Requirement' exercise should take place with relevant stakeholders and its outcome should be used for the design, performance specification, management and functionality of the CCTV system. In effect, it is a statement of problems, not solutions and will highlight the areas that must be observed by the system and the times and description of activities giving cause for concern. A useful reference to help achieve this goal is the CCTV Operational Requirements Manual 2009 ISBN 978-1-84726-902-7 Published April 2009 by the Home Office Scientific Development Branch available at this link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf

16.4 Strategic CCTV - University Security Services

University Security Services manage, record and monitor a number of CCTV cameras located across the University estate. OUSS are developing CCTV plans in line with Masterplans for a number of different areas and these are available from the CPDA. The aim, where possible, is to building mount these cameras and the cost of the installation of these cameras will be absorbed by the appropriate Capital Project. The CPDA will advise the Project Manager if OUSS strategic CCTV cameras will be included in the building design. OUSS will take on the servicing and maintenance of these identified cameras once they are commissioned.

CCTV - Technical information see Section 24 of this document

16.5 Department options: Estates CCTV network

The University of Oxford have recently installed a fully IP digital recording solution. This platform provides the University with an open protocol system with the ability to integrate more than 24 camera manufacturer's equipment. Department(s) will have the option to install a standalone CCTV system or to join the University CCTV system. New department installed CCTV systems should be installed so that their systems are compatible with the wider University CCTV scheme to allow departments, post-occupation, to join the University scheme if they later choose to. The below points should be considered:

- All new CCTV systems installed should have IP network cameras
- All new cameras must be form the approved list held by OUSS
- The maintenance provider for OUSS will provide the relevant camera licences and facilitate the camera integration onto the University digital system.

Charges will apply contact the Operations Manager at Security Services for further information.

16.6 The University Security Policy

Requires all of its buildings to have a Security Plan which includes a 'CCTV Standards and Procedures' document that must be completed by the end users when the CCTV system is handed over. Available at this link: http://www.admin.ox.ac.uk/ouss/

16.7 Data Protection

Further information to ensure your CCTV is compliant with the Data Protection Act 1998 can be found at this link:

https://ico.org.uk/for-organisations/guide-to-data-protection/cctv

16.8 Camera Surveillance Commissioner (CSC) Code of Practise

In 2013 the CSC issued 12 guiding principles for operating CCTV in public places and these codes, although not mandatory for education establishments at this time, should be considered by the end user. CCTV systems must be justified with a legitimate reason and pressing need for its installation. The University CPDA can offer advice, support and guidance in relation to this. Details can be found at this link:

https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

17. Building envelope

This section includes wall construction, glazed curtain walling and window walls, roller shutters and grills, roof construction, roof lights and sun tubes, external doorset apertures, locks for doorsets and gates, glazing within doorsets and secure vision panels protecting window apertures, secondary glazing, security glazing, access control, keyless buildings, and entrance barriers.

17.1 Wall construction

Due to the remoteness of some building locations and/or reduced activity at night and over the weekends some buildings become prone to criminal attack through the wall or roof thus by-passing security doors and shutters. The walls should therefore be designed to withstand such attacks and materials resistant to manual attack or damage should be used to ensure the initial provision of security.

Where lightweight construction is being considered, for example the use of insulated sheet cladding, a reinforced lining such as welded steel mesh and/or the installation of an internal 2.2 metre high block walling can improve the security of the building walls.

17.2 Glazed curtain walling and window walls

There are four distinct types of glazed wall systems. These are:

- Large glazed units connected by a 'spider clamp system'.
- Glazed units directly retained within a framing system (usually aluminium).
- Framed windows installed within a separate framing system.
- Framed windows connected to other framed windows to create a 'window wall'.

Glazed curtain walling must be installed using a secure glazing retention system. The method of retaining the glass must include one or more of the following:

- Security glazing tape.
- Dedicated security sealant or gasket.
- A secure mechanical fixing system.

One pane of laminated glass minimum thickness 6.8 mm, tested to BS EN 356:2000 P1A is recommended in these structures.

17.3 Roller shutters and grilles

Grilles and shutters can provide additional protection to both internal and external doors and windows. The minimum standard are products tested and certified to:

- LPS 1175 Security Rating 1
- STS 202 Burglary Rating 1

The CPDA or Insurers will determine whether a higher security rated roller shutter or grill is required by referring to the current and perceived risk, threat and vulnerability levels.

Roller shutter doors providing access for deliveries and other apertures where no other door is present should be certificated to a minimum standard of:

- LPS 1175 Security Rating 2
- STS 202 Burglary Rating 2

The CPDA or Insurers will determine whether a higher security rated roller shutter or grill is required by referring to the current and perceived risk, threat and vulnerability levels.

17.4 Roof construction

Roofs are vulnerable to criminal intrusion and damage through vandalism, therefore careful consideration must be given to their construction.

Lightweight roofing systems should be certified to a minimum security standard of LPS 1175 Security Rating 1

Where roofing systems, other than lightweight, are to be installed potential for criminal intrusion of decking below a membrane should be considered. Metal decks, particularly steel, may be more resistant than timber. Expanded metal or welded mesh between the skins of double-skinned roof coverings or within the roof space may be considered for timber decks.

Vulnerable ceiling voids may need to be protected by a monitored Intruder Detection System (IDS).

17.5 Roof lights and sun tubes

Roof lights must be securely fixed in accordance with the manufacturer's specifications. Based on a site specific risk assessment by the CPDA which will take into account contributing factors such as the accessibility and visibility, a roof light aperture may need to be protected by either one, or a combination of the following:

- In low risk applications a roof light aperture should be protected by roof lights certificated to LPS 1175 Security Rating 1 or STS 202 Burglary Rating 1
- In higher risk applications a roof light aperture should be protected by roof lights certificated to LPS 1175 Security Rating 2 or 3 or STS 202 Burglary Rating 2 or 3
- Alternatively, a roof light may be used in conjunction with an internal grille certificated to LPS 1175 Security Rating 1 or STS 202 Burglary Rating 1

To prevent large dimension sun tubes being used to gain access into a building ensure that the caps on those that are easily accessible are effectively secured.

17.6 External door apertures

It is important that external doorset apertures are protected. The normal expectation is that ground floor and easy to reach doors will be tested and certified to one of the following standards:

- PAS 24: 2016
- STS 201 or STS 202
- LPS 1175 SR1 Security Rating 1
- LPS 2081 Security Rating A

Due to the nature of some department activities physical security standards may need to be higher, this may be achieved through the use of additional protection such as a roller shutter or a grille as described in section 18.3 or through the use of higher security rated doors. A requirement for external doorsets to be certified to a higher standard of security will be determined by the risks, threats and vulnerabilities identified by the CPDA or Insurers.

All external entrance doors should be fitted with a key operated physical lock to facilitate a managed building lockdown or to secure a building in the event of an extended power failure.

Where possible external doors should not be recessed more than 600mm from the building elevation.

Multiple exit doors: - Fire escape and occasional use doors, should be protected by door contacts to indicate to reception staff/OUSS if a door is left open or ajar longer than necessary. In certain circumstances where exit doors are in an isolated location the addition of a screech alarm is recommended to draw attention to the open door.

Electronic Locks: If external doorsets are secured with electronic plates, the magnetic plates at the top of the door(s) should have a holding force of 7KN, 713kgs or 1570lbs. An additional electronic strike plate should be incorporated half way down the doors edge to reduce the amount of movement of the door in its frame.

Outsized or bespoke door designs: It may not be possible to obtain security rated doors if they are oversized or a bespoke design, or on a listed building in these circumstances the following physical security measures should be considered:

- A solid core door: Minimum 44mm thickness, fitted with 2x 5 lever mortise door locks installed at to BS 3621 or BS 8621, 2x hinge pins on each door leaf and a view finder or vision panel.
- Double doorsets: The design of double doorsets can create building insecurities, where doors meet in the middle and in the absence of a central supporting frame there is often excessive movement of the doors which provides an opportunity for the doors to be prised open. When installing a double doorset secure one door leaf using a physical bolt system to secure the top and bottom of the slave door in place and install hinge pins on each door leaf
- Sliding doors: External sliding entrance doors that meet in the centre create security weaknesses for buildings, it is relatively easy to prise these doors apart. Incorporate an integrated door locking mechanism within the frame of the sliding doors, this usually has to be specified at the time of placing the order for the doors.

Other door designs should be referred to the CPDA for physical security recommendations.

17.7 Lock security standards for doors and gates

The below table provides the current single point locking, multi-point locking and dual mode locking standards. Please note that dual mode locks type BS/PAS 10621 must only be specified for use within buildings that have alternative means of escape.

Lock Standard	Application	Features
BS 3621 : 2007	Single point locking	Key entry to key egress
BS 8621 : 2007		Key entry to thumb turn Egress
BS 10621 : 2007		Dual mode: Lock by key outside only; can be opened from inside without a key EXCEPT when this function has been disabled by a positive key operation from the outside.
PAS 3621-2 : 2009	Multi point locking	Key entry to key egress
PAS 8621-2 : 2009		Key entry to thumb turn egress
PAS 10621-2 : 2009		Dual mode: Lock by key outside only; can be opened from inside without a key EXCEPT when this function has been disabled by a positive key operation from the outside.
EN 1303	Cylinder lock	Grade 5 Key security Grade 0 Attack resistance Grade 2 Drill attack resistance
DHF TS 007 3* standard	Replacement cylinder Lock	Enhanced security performance for replacement cylinders and/or security hardware

NOTE: Retrospective replacement of key cylinders should be configured to security standard DHF TS 007 + A2: 2018 3*(three star)

17.8 Glazing within doorsets and secure vision panels

All glazing in and adjacent to doors including vision panels must include one pane of laminated glass minimum thickness 6.8mm and successfully tested to BS EN 356: 2000 P1A

Secure vision panels - Where privacy is required, together with a degree of security, both external and internal doorsets can be fitted with a secure vision panel. Secure vision panels allow for the control of vision into a private area or room or for views of an outside area for the purpose of manual visual access control. The vision panels should match the security rating of the door.

17.9 Window apertures

It is important that external ground floor and easy to reach windows apertures are protected. The normal expectation is that ground floor windows will be tested and certified to one of the following standards:

- PAS 24: 2016
- STS 204
- LPS 1175 SR1 Security Rating 1
- LPS 2081 Security Rating A

Due to the nature of some University Department activities and uses physical security standards may need to be higher, this may be achieved through the use of additional protection such as a roller shutter or a grille as described in section (18.3) above or through the use of higher security rated security windows.

All glazing in windows that are easily accessible must include one pane of laminated glass minimum thickness 6.8mm and successfully tested to BS EN 356: 2000 P1A.

It may be necessary to restrict the opening or ground floor and easy to reach windows to 100mm this should be achieved by using a quick release window restrictor.

17.10 Secondary glazing

The security of standard windows can also be improved through the use of security rated secondary glazing systems, certified to:

- PAS 24: 2016
- STS 204
- LPS 1175 Security Rating 1
- LPS 2081 Security Rating A

17.11 Glazing (laminated glass)

All ground floor and easily accessible glazing should incorporate one pane of laminated glass minimum thickness 6.8mm and successfully tested to BS EN 356:2000 P1A.

The below table shows the P rating and Glass thickness in Standard BSEN356:2000

Low resistance Level

BS EN356 - P1A, 6.8mm	BS EN356 - P2A, 8.1mm	BS EN356 - P3A, 8.5mm
BS EN356 - P4A, 9.5mm	BS EN356 - P5A, 10.3mm	

High resistance Level

BS EN356 - P6B	BS EN356 – P7B	BS EN 356 P8B

11mm Glass PVB 18mm Glass Poly Glass	11mm Glass PVB 28mm Glass Poly Glass	36mm Glass PVB 13mm Glass Poly Glass

The CPDA will assess the risks, threats and vulnerabilities to a building to justify the use of laminated security glazing to security standard LPS1170, this standard of laminated glazing is recommended when replacing glass in doors and windows tested to security standard LPS1175.

18. Access Control

An access control strategy should be developed at an early stage and building a new premise presents the ideal opportunity to design in an integrated access control system to control identified external and internal doorsets. Access control system must be supported by robust management to ensure its effectiveness.

Early discussions with the CPDA and the intended building occupier may indicate the level of access control required for each room, corridor, floor and even the lifts. This information should be used to develop the access control strategy.

18.1 Electronic access control

Electro-magnetic locks can vary tremendously in type, cost, security and general performance. Please view the below link to the British Security Industry Association guide to:

https://www.bsia.co.uk/Portals/4/Publications/132-specifiers-guide-access-control-systems[1].pdf

The need for access control will be influenced by many factors including the following:

- The need to protect a lone worker or vulnerable persons working in a reception area.
- To prevent access into parts of the building beyond the reception to prevent crime and maintain health and safety.
- To prevent trespass onto offices, vulnerable rooms and research areas, especially where the offices and the reception are located on an upper floor.
- Type of business or business practices.
- Local risk, threats and vulnerability factors.
- Where two or more departments share a common entrance. In all such cases the doors should incorporate an electronic access control system, with an electronic lock release and (for the main entrance) and where departments share a common entrance an audio visual unit should be installed to facilitate communication from the main entrance to the individual department or reception areas.

18.2 Keyless buildings

It is recommended that key operated physical locks are fitted onto final exit doors, this would facilitate a building lockdown or secure an unoccupied building in the event of complete power failure and back-up battery failure. **Further advice should be sought from the University Fire Officer if these doors form part of a fire escape route.**

An integral key code entry pad will provide a second level of security to access buildings out of usual working hours or into restricted or high risk areas.

Holding Force: The trending for keyless buildings can mean that the perimeter security is totally reliant on electronic locking mechanisms as opposed to physical locks. Where the security of a door relies on magnetic plates alone it is essential to consider an appropriate holding force for the magnetic plates, if the holding force is low then it is relatively easy to apply force to the door separating the two magnetic plates allowing unauthorised access into the building. It is recommended for external entrance/exit doors that either one lock of 7KN (1570lbs, 713kg) holding force or 2x locks of 5KN (1125lbs, 509kg) holding force are fitted to the door. Additionally an electronic strike plate should be incorporated half way down the doors edge to reduce the amount of movement of the door in its frame.

Seek advice from the University Facilities Management Department at Estates Services for information on preferred access control systems.

18.2 Magnetic locks and fire alarm activation.

Magnetic locks are designed to 'fail' to facilitate the safe escape of people from the building. Security provision for final exit doors should never compromise the fire escape routes. Magnetic locks are designed to react to a fire alarm activation and the following agreed terminology describes their reaction:

- Fail Safe Open = doors automatically open when the fire alarm sounds
- Fail Safe Shut = the doors automatically unlock when the fire alarm sounds, but they do not automatically open
- Fail Safe Locked = the doors remain locked when the fire alarm sounds and need to be released by pushing the green mushroom exit button or the green emergency door release unit, thumb-turn or other mechanical lock or push bar / push handle

Be aware pushing the green emergency door release unit means the doors will remain unlocked until the unit is reset using a key. This does create a security weakness for the building.

All green emergency door release units should be fitted with a protective plastic cover the reduce incidents of accidental use. The emergency door release units can be fitted with an alarm system that sounds when it is pushed to draw attention to an accidental activation by building occupants.

Where possible incorporate a traditional manual fire escape door push bar, small push handle, thumb-turn egress which will manually disengage the holding bolts of the fire door. Allowing them to re-engage once the door has closed shut.

Fire escape doors should always be protected by the building alarm systems so that a signal is sent back to the reception and or University Security Services to indicate if a door has been propped open longer than usual. If doors are in an isolated location the installation of an additional screech alarm should be considered.

18.4 Entrance barriers

The major difference between turnstiles and doors is that they restrict passage, usually allowing only one person to pass at a time. They can also enforce a single direction of passage and can stop people that have not presented correct identification. Turnstiles are used in a variety of locations such as libraries, main or secondary entrance doors, office lobbies and controlling access around a building shared by different departments.

As a security feature some turnstiles offer much greater security than others. For example a full height turnstile can hinder a person from gaining access at an unattended location whereas a half-height turnstile can be jumped over. The latter may be suitable in a reception area where reception staff can monitor access through the turnstile.

When considering the use of turnstile type barrier the following features should be considered to inform the type of barrier you require.

- How easy and obvious should it be to use?
- How will the turnstile be supplied, delivered and erected?
- How easy is it to supply power to the turnstile?
- Is appearance important?
- How fast should it operate? The slower the throughput, the more lanes will be required.
- How many lanes are required? Will they fit in the available space?
- Will the restrictions of the turnstile need to be removed from time to time or are there alternative routes?
- Would the turnstile prevent access or exit in the case of a fire?
- How tall should it be (to prevent jumping or climbing)?
- How strong should it be? How high a force should it resist?

If the turnstile/barrier forms part of the building fire escape strategy the University Fire Officer must be consulted

18.5 Trade Buttons

A feature of some academic and residential buildings is the provision of an audio or audio visual intercom system to get access. The installation of a trade entry button on the intercom units should not be considered as this causes an unnecessary vulnerability to building security.

18.6 Thief resistant electronic door locking devices

Thief resistant electronic door locking devices – Standard DHF TS 621:2018 addresses vulnerability of radio frequency network and vulnerability of devices.

19. Mail and parcel delivery

For the majority of academic buildings it is expected that mail delivery will take place during normal office hours using the University Messaging Service or that mail and parcel deliveries will be handed into reception.

The storage of delivered parcels at a centralised collection point needs to be in a secured office or cage, and there needs to be robust management of a receipt signing process to avoid parcels being misplaced, misdirected or stolen.

Letter plate apertures are associated with crimes such as arson, lock manipulation and fishing (removing mail from the letter box through the letter aperture from outside) therefore it is strongly recommended that out of hours delivery is via a secure external letter box or ‘through the wall’ into a secure area.

Where an external mounted letter box is being used it must be:

- Robust in construction.
- Securely fixed to the external face of the building as per manufacturers’ instructions.

- It must be located in a position that benefits from natural surveillance.
- The letter box design must prevent the removal of mail through the delivery slot.
- The access door must be lockable.

Letter Boxes certified to Door & Hardware Federation specification TS009 (DHF TS 009) provide a safe and secure way for mail to be delivered.

Where 'through the wall' mail delivery is being used then all the above attributes should be considered but the installation of a Letter Plate certified to Door & Hardware Federation specification TS008 (DHF TS 008) will provide greater reassurance that this type of mail delivery offers similar security attributes as letter boxes certified to TS009

20. Internal security considerations

This section reviews the security standards and other considerations for intruder detection systems, fogging devices, vulnerable rooms, internal doorsets and student lockers.

20.1 Intruder Detection System (IDS)

University Security Services can provide alarm monitoring services please contact the Operations Manager for further information on monitoring station standards and service charging.

Alarm monitoring – Technical information - see Section 25 of this document

An intruder detection system strategy should be developed at an early stage in the building design.

A suitably designed, fit for purpose and monitored intruder detection system should be installed, and where a police response is required, the system must comply with the requirements of the Associations of Chief Police Officers (ACPO) Security Systems Policy. The CPDA can provide advice and guidance on the police alarm attendance policy.

European Standard EN50131 for intruder detection systems evaluates the risk associated with the premises and determines the grade of system required. Each alarm grade is described in terms of the type of intruder and how much effort they would put into a burglary. The appropriate intruder alarm grading is usually determined by the Insurers. A grade 3 alarm is usually recommended.

The below table illustrates the intruder alarm grades 'v' risks:

Grade	Risk/Threat/Vulnerability	Type of attack and knowledge of offender
Grade 1	Low risk of theft	The property is not likely to attack intruders. It is assumed that a thief is likely to be opportunist rather than bothering to plan things in advance and that the intruder is simply going to break open a door.
		The property is likely to have something of interest to an experienced thief. The intruder is expected to have some knowledge of how alarm systems work and possibly carry some tools to allow them to

Grade 2	Slightly higher risk of theft	overcome a simple alarm system. The thief is likely to check the building for ease of access through doors, windows and other openings.
Grade 3	Substantial risk to property.	There is a good reason to assume it may be broken into and might well contain objects of high value. An intruder is likely to get access by penetrating doors, windows or other openings. The thief could be very experienced with intruder alarms systems and possess a number of tools and equipment to overcome the system
Grade 4	Very high risk properties	Intruders could be expected to plan a burglary in advance and have the knowledge and equipment to alter parts of the intruder system to prevent detection. It is assumed that the intruder could gain access by penetration of floors, walls and ceilings. The intruder is unlikely to be working alone.

20.2 Security fogging devices

Security fogging and offender marking systems can be included within an intruder detection system to disorientate or mark an intruder if the alarm system is activated. They must confirm to BS EN 50131-8:2009 Alarm Systems Security fog devices/systems.

20.3 Public address systems

Public address systems provide instant, effective communication to all staff members particularly in emergency situations where a prearranged and rehearsed response to particular situations can be initiated.

20.4 Physical security standards for vulnerable rooms.

Consideration must be given to the structure of the internal walls, floors and ceilings of vulnerable rooms, so that appropriate security is provided to protect the contents of the room/area. Combinations of different materials, such as high impact gypsum boards, expanded metal sheets, plywood, and masonry have proved to be effective in upgrading the security of walls, floors and ceilings.

The physical security standards required for Laboratory areas must be specified by the University Safety Office.

20.5 Internal doorsets

There is a minimum physical security standard for internal security rated doors (see section 17.6)

In certain locations where security levels may need to be higher the CPDA or insurers will assess the risks, threats and vulnerabilities and recommend a suitable security standard.

20.6 Student lockers

It is preferable to locate student lockers in areas that have high circulation and passive surveillance. Where located along corridors lockers must be non-combustible.

21. Soft Landings – University Security Services

University Security Services (OUSS) provide safe environments by offering response, prevention and reassurance to staff students and visitors. At building handover OUSS may take on the responsibility of Security monitoring and response and as such require a number of measures to be put into place between practical completion and building handover.

- Intruder alarms must be operating without false activations for a period of 24 hours before handover.
- Fire Alarms must be operating without any false activations for a period of 24 hours before building handover.
- The incoming department must inform Security Services of the contact details for building key holder's
- Security Staff must be trained in the operation of the building IDS and Fire alarm.
- CCTV – (see section 23) - If there is a requirement for Security Services to monitor CCTV the appropriate IT connections should be active and operational before building handover.

22. Security standards

BS 5489:2013 – *External lighting standard*

BS EN 356:2000 – *Laminated glass standard*

LPS 1270 – *Glazing standard - Developed to ensure protection against terrorist or determined criminal attack.*

LPS 1175 - *Physical security standards for non-domestic building components, strong points and security enclosures*

LPS 2018 - *Similar standard to LPS 1175 but relates specifically to intrusion by stealth attack*

STS 201 - *Enhanced security requirements for doorsets*

STS 202 – *Requirements for burglary resistance of construction products inducing hinged, pivoted, folding or sliding doorsets, windows, curtain walling, security grills, garage doors and shutters*

STS 204 - *Enhanced security performance for windows*

PAS 24: 2016 – *Door and window security standard*

PAS 68-1:2007 - *Fixed and rising security standard bollards.*

PAS 69: 2006 - *Provides guidance on the appropriate selection, installation and use of such bollards.*

IWA 14 - *is the International Workshop Agreement which specifies the essential impact performance requirement for a vehicle security barrier (VSB) and a test method for rating its performance when subjected to a single impact by a test vehicle not driven by a human being.*

DHF TS 007: 2012 + A2 2018 – *Security rated replacement cylinder lock - 3* rating*

DHF TS 008: 2012 – *Security letter plates*

DHF TS 009: 2012 – *Security letter boxes*

DHF TS 261:2018 – Thief resistant electronic door locking devices

BS 3621: 2007 - *Single locking point key entry to key egress lock*

BS 8621: 2007 - *Single locking point key to thumbturn egress lock*

BS 10621: 2007 - *Single locking point dual lock*

PAS 3621: 2009 - *Multi locking point key entry to key egress lock*

PAS 8621: 2009 – *Multi locking point key entry and thumbturn egress*

PAS 10621: 2009 – *Multi locking point dual lock*

Sold Secure - *Bronze (lowest), Silver and Gold (highest) security standards.*

EN 50131 – *Intruder Detection System and hold up alarms*

LPS 1654/BSEN12302/CEN & Sold Secure – *Padlocks*

23. Strategic CCTV – Technical Information – Author Mark Round Estates IT Manager
Service Owner: Security Services.

Service stakeholders: Security Services, Systems Manager, Network Manager

Network to use: ESTSN Secure Network

Current Maintainer: Tyco

Overview
Security Services operates and maintains a strategic CCTV solution for the University. The system covers a range of locations across the city to provide assistance to historical and real time events. This documents relates to the technical aspects of camera compatibility and connectivity. For advice and guidance on camera locations and specifications please contact security services.

NB: CCTV solutions in a department are the responsibility of the department and do not form any part of this service. If there is a need to share CCTV with Security Services a separate design process needs to be initiated.

Hardware and Software

The current system in place is provided and maintained by current maintainer. The system is based on the Latitude solution from FLIR. All communications to the system are Internet Protocol (IP) based and all feeds should either be direct from compatible cameras or encoders. Security Services can provide a detailed list of current compatible devices. This list is regularly updated so please request the current version before selecting cameras.

Unless otherwise stated, all internal CCTV cameras should be powered by Power over Ethernet (PoE) and external cameras should be powered by a separate mains electrical supply just before the connection leaves the building.

Network Connectivity

All CCTV feeds will be connected to the ESTSN Secure network. Delivery of this network within buildings will be with agreement of local departmental IT staff.

Responsibilities

The following table shows responsibilities for the installation / commissioning of centrally managed cameras:

All cameras / encoders will be supplied, installed and configured by an existing supplier as stated in Annex I

All cameras / encoders will be maintained by Security Services via the current maintainer.

Hardware warranty issues will be identified by current maintainer

Hardware warranty replacement / support will be carried out by chosen supplier / installer.

Design Considerations

Network Connectivity – 1No. Cat6a data points should be installed to each CCTV camera / encoder installation location within 0.5m of the connection point and should be suitably secure from disconnection (.e.g. locked cupboard/ box).

Power – Power to internal cameras should be delivered by Power over Ethernet (PoE) If the Camera is external a MK Electrak Socket should be installed within 0.5m of the point where the connection leaves the building.

Variation

Any variation from the above must be approved by both the service owner and the service stakeholders.

Costs

All installation and setup costs are the responsibility of the building / department / project. Ongoing maintenance may be charged depending on whether the camera is of strategic importance to the University.

Any costs associated with obtaining approval for devices not listed on the compatibility list are the responsibility of the building / department / project. Approval can only be completed by the current maintainer and will be at the cost quoted by them.

Contacts

Supply, install and configuration: see Appendix I

Approval to connect to the service, and ongoing monitoring and maintenance: Security Services (securityservices.updates@admin.ox.ac.uk)

Further information
https://www1.admin.ox.ac.uk/ouss/cctv/

Appendix I - Current Suppliers

Chris Lewis Fire and Security, Contact Security, Tyco

24. Alarm Monitoring – Technical Information – Author Mark Round Estates IT Manager

Service Owner: Security Services.

Service stakeholders: Security Services, Systems Manager, Network Manager, University fire officer

Network to use: ESTSN Secure Network

Overview
All relevant building alarms should remotely report to Oxford University Security Services alarm monitoring service. This service is designed as an early warning system for the University and does not form any formal part of legislative compliance / standards for fire and intruder alarms.

Hardware and Software
The current system in place is provided by DRAX Technologies Ltd and maintained by Tyco / ADT. Security Services run a number of AMX central alarm receiving stations and alarms are received from a number of different versions of remote alarm transmitters.

The current standard device that will be installed is the SMaRT Watch module from DRAX Technologies Ltd.

Traditionally alarm signals from various devices were concentrated toward a single panel device (DRAX Panel) within a building. Given the nature and size of the **SMaRT Watch** device, multiple devices can be installed in a building and connected to the relevant network.

Network Connectivity
All SMaRT Watch nodes will be connected to the ESTSN Secure network.

Responsibilities
The following table shows responsibilities for the process / deliver of alarm monitoring:

All modules will be supplied by: Pyrotec

All modules will be installed by: Pyrotec

All module configuration will be carried out by: Pyrotec

All monitoring station configuration will be carried out by: Tyco / ADT

All maintenance of the device will be carried out by: Tyco / ADT

12 month hardware warranty issues will be identified by Tyco / ADT

12 month hardware warranty replacement / support will be carried out by: Pyrotec / DRAX

Design Authority
Pyrotech as the certified and manufacturer supported installer of the product will be the final design authority.

Design Considerations
Enclosure – The SMaRT Watch module can be installed in some alarm systems but is also installable in its own housing.

Network Connectivity – 2No. Cat5e data points should be installed to each SMaRT Watch installation location within 0.5m of the SMaRT watch and should be suitably secure from disconnection (.e.g. locked cupboard/ box). If the module is being installed in an existing alarm, the data point termination can also be within the alarm panel.

Power – If the SMaRT watch is being installed standalone, a MK Electrak Socket should be installed within 0.5m of the installation.

Variation
Any variation from the above must be approved by both the service owner and the service stakeholders.

Costs
All installation and setup costs are the responsibility of the building / department / project. Ongoing maintenance may be charged depending on the nature of the alarms being monitored.

Contacts
Supply, install and configuration: Pyrotec (mail@pyrotec-systems.co.uk)

Approval to connect to the service, and ongoing monitoring and maintenance: Security Services (securityservices.updates@admin.ox.ac.uk)

25 The Checklist

This checklist is designed to guide you through a two stage process for incorporating best practise crime prevention features within the development. The number in brackets at the end of each bullet point refers to the corresponding section within the main philosophy document which provides further information or explanation.

- *The University Crime Prevention Design Advisor has been consulted.*

- *The Design and Access Statement demonstrates that the design of the development has taken Crime Prevention into consideration and reflects the 7 attributes for creating safe and sustainable environments(1.2 & 3)*

Design and Layout

- *The site demonstrates clear distinction between private and public areas (4.1)*

- *Buildings are orientated to maximise opportunity for natural surveillance from other buildings and vice versa (4.3)*

- *Outdoor amenity spaces and socialising areas are well designed and overlooked by buildings (4.4)*

Roads and paths

- *The security of the development is not compromised by excessive through routes (5.1)*

- *All vehicle, pedestrian and cycle routes visually open, direct and well used (5.2)*

- *The pedestrian and cycle routes are not unnecessarily segregated. Isolated routes are straight, wide, well lit (if appropriate) and avoid potential hiding places (5.3)*

- *Planting next to buildings or footpaths does not create hiding places or obstruct surveillance opportunities (5.4)*

- *Where appropriate, all pedestrian and cycle routes are illuminated. (5.5)*

Perimeter

- *Where appropriate the design creates a secure site (6.1)*

- *All boundaries are clearly defined by psychological, controlling or security demarcation (6.2)*

- *Fencing has been considered and all the entrance gates are of the same standard as the fencing (6.3 & 6.4)*

- *Defensive planting has been considered to enhance boundary security and control movements through the site (6.5)*
- *Building locations, reception areas and parking areas are clearly signposted (6.6)*

Vehicle Parking – Cars, bicycles and motorbikes

- *Natural surveillance has been considered in the design of the parking areas (7.1)*

- *Secured delivery and collection of goods areas have been considered (7.2)*

- *Multi-storey, surface and underground parking facilities demonstrate best practise features (7.3, 7.4, & 7.5)*

- *Motorcycle parking has been considered (7.6)*

- *Long and short term cycle parking is located within sight of occupied buildings, has appropriate cycle parking stands, is illuminated overnight and incorporates best practise design features (7.7)*

External Lighting

- *An external lighting strategy has been developed which does not conflict with the CCTV or Landscape strategies. External lighting does not create dark shadowed areas and incorporates best practise guidance. (8)*

- *All external lighting is effective and fit for purpose (8.1)*

- *Bollard style lights and feature lights are not security lights and are supported by additional lighting provision (8.2 & 8.3)*

- *Motion sensitive lighting is fit for purpose and suitable for the surrounding area (8.4)*

- *All observable elevations, main entrances and parking areas are illuminated during the hours of darkness (8.5)*

External security issues

- *A Landscape strategy has been developed and does not conflict with CCTV and Lighting Strategies. Hiding places have been avoided and opportunities for surveillance have been considered (9.1)*

- *External furniture and litterbins are designed to reduce opportunity for misuse. They do not provide climbing aids and are secured to the ground (9.2)*

- *All recessed areas are designed out or are overlooked by other buildings. Where appropriate external doors are fitted with security rated doors, grills or shutters (9.3 & 17.3)*

- *The number of recessed external doors has been kept to a minimum. Where possible external doors are recessed no deeper than 600mm into the building elevation (9.3 & 17.6)*

- *Temporary buildings are secure and voids under the buildings are enclosed (9.4)*

- *Wind turbines and photovoltaic installations have been located to minimise the risk of damage. (9.5)*

- *If appropriate heating, ventilation and air conditioning units are located at level 2 or above. (9.6)*

Internal and external storage facilities

- *All cleaners cupboards/rooms are lockable (10.1)*
- *All external non-hazardous waste 'wheeled' containers are located away from hazards and are lockable (10.2)*
- *All hazardous waste storage has been considered and referred to the Hazardous Waste Technician at the University Safety Office (10.1 & 10.2)*

Utility Services

- *All telecommunication and utility access covers are secure (11.1)*
- *Access to the Utility meters does not compromise building security (11.2)*

Building Shell

- *Windowless building elevations are protected against crime (12.1)*
- *Automatic opening windows are designed so that the building security is not compromised (12.2)*
- *The design of the building facades minimise the opportunity for hiding and climbing up to windows and roofs. Climbing aids such as boundary walls, deep windows sills, drain pipes and external staircases have been designed out. (12.3 & 12.4)*

Internal layout

- *The main building entrance(s) are clearly visible from reception (13.1)*
- *Additional entrances are monitored by CCTV at reception and/or controlled by internal entrance barriers (13.2 & 13.3)*
- *The reception desk and surrounding area is designed to protect the staff and reduce opportunity for assault on staff. The design has incorporated the good design features (13.3 & 13.4)*
- *An access control strategy has been developed and identified internal doors are fitted with access control or physical key locks.(13.5)*
- *Critical areas including entrance foyers, corridors, staircases and landings are illuminated during the hours of darkness and, where appropriate, movement activated lighting is installed throughout the building (13.6)*

Physical Security

- *Minimum physical security standards are incorporated in this design and meet the insurance providers requirements(14)*

Perimeter – high security

- *The need for security fencing has been considered for the development (15.1)*

- *Security gates providing access down the side of buildings are security rated, as specified, and constructed as anti-climb designs. Gates are the same security rating as the fence (15.2)*

- *The need for security rated bollards, as specified, has been considered (15.3)*

- *Padlock standards (15.4)*

Closed Circuit Television (CCTV)

- *An external CCTV strategy has been developed to avoid conflict with the lighting and landscape strategy (16.1)*

- *Standalone CCTV systems (16.2)*

- *A CCTV Operational Requirement exercise has been carried out by the end user to ensure the proposed CCTV system is fit for purpose and compliant with Data Protection Act 1998 (16.3 &16.7)*

- *Strategic CCTV cameras – University Security Services (16.4)*

- *Strategic CCTV – Technical Information (16.4 & 23)*

- *Department Options: Estates Services CCTV network, ORION platform (16.5)*

- *University Security Policy – end user to complete the CCTV Standards and Procedures document (16.6)*

- *Camera Surveillance Commissioner (CSC) Code of Practise – has been considered by the end user (16.8)*

Building envelope - security

- *The building walls have been designed to withstand attack, lightweight constructed walls have been reinforced with welded mesh sheets or internal block walls. (17.1)*

- *Glazed curtain walling or window walls have been installed using security tape, dedicated security sealant or gasket or a secure mechanical fixing system. All glazing should incorporate laminated security glass. (17.2 & 17.11)*

- *All security roller shutters and grills are tested and certified to minimum security standards as specified (17.3)*

- *Lightweight roof systems are tested and certified to minimum security standard as specified (17.4)*

- *Low level and easy to reach roof lights and sun tubes are protected by appropriate security measures (17.5)*

- *All external door apertures are protected by doors that are tested and certified to the minimum security standard as specified and fitted with a key operated lock (17.6)*

- *Non-standard or bespoke design doors (17.6)*

- *All non-security rated door and gate locks should be fitted with minimum lock security standards as specified (17.7)*

- *All glazing in and adjacent to doors incorporates one pane of laminated security glass (17.8 & 17.11)*

- *All ground floor and easy to reach windows are tested and certified to the minimum security standards as specified (17.9)*

- *Where appropriate all ground floor and below ground floor secondary glazing units should be tested and certified to minimum security standards as specified (17.10)*
- *All ground, below ground level and easy to reach windows should incorporate one pane of laminated security glass. (17.11)*

Access control

- *An access control strategy has been developed taking into account emergency egress requirements, vulnerable rooms, doors, lifts, corridors and other areas. (18.1)*

- *Physical key locks have been fitted to secure final exit doors, taking into account emergency egress requirements (18.2)*

- *Magnetic locks have the appropriate holding force, as specified (18.2)*
- *Magnetic Locks and fire alarm activation (18.3)*
- *Entrance barriers have been considered where passage needs to be controlled or restricted. They provide an appropriate level of security (18.4)*

- *Trade buttons are not provided for trade persons access (18.5)*

- *The vulnerability of locking devices radio frequency network and vulnerability of devices has been addressed (18.6)*

Mail delivery

- *Secure storage for delivered parcels has been provided (19)*

- *Out of hours mail delivery will be into an external mail box or through the wall into a secure area as specified (19)*

Internal security considerations

- *An intruder detection system (IDS) strategy has been developed, and the alarm grading is appropriate to the risk. (20.1).*

- *Alarm Monitoring -Technical information (24)*

- *A public address system has been considered (20.3)*

- *Vulnerable rooms have been identified and where appropriate 'security rated' internal doors have been specified. The walls and ceilings to these rooms are of the same security standard. (20.4, 20.5 & 17.6)*

- *Student Lockers are non-combustible and have been located in areas of high circulation.(20.6)*

Soft Landings – University Security Services
At building handover Security Services may take on the security of the building in these cases the following applies:

- *The intruder detection system is operating without fault for 24 hrs before building handover (21)*
- *The fire alarm system is operating without fault for 24 hrs before building handover (21)*
- *Security Services MUST have the department personnel call out details before building handover (21)*
- *Security Staff have been trained in the operation of the building IDS and Fire Alarm panels (21)*
- *CCTV – strategic cameras are operating and capable of being viewed at Security (21)*