



CRIME IMPACT STATEMENT

ICON INDUSTRIAL UNIT 2, SUNBANK LANE, MANCHESTER
INDUSTRIAL & ANCILLARY OFFICES (OPTION 1 - 49,192sqm
or OPTION 2 – 36,975sqm.)

Greater Manchester Police

designforsecurity

FOR: Icon Manchester Developments Ltd.

VERSION A: 04/07/19

REFERENCE: 2019/0469/CIS/01

Icon Industrial Unit 2, Sunbank Lane, Manchester

URN: 2019/0469/CIS/01

EXECUTIVE SUMMARY

Minor design changes/security additions required

This development has been assessed against the principles of 'Crime Prevention Through Environmental Design' (CPTED), in order to reduce the opportunities for crime and the fear of crime. Particular consideration should be given to the boundary treatments, including enclosure and protection to the sides and rear of the building (including service yards and parking areas) and the control of access into/around the site and the building itself, which is discussed in more detail within Section 3.3 of this report:

If these issues can be addressed as described within the report and the other physical security measures are incorporated, I would be happy to support the development.

Please note: Greater Manchester Police Design for Security will recommend to the local planning authority that a planning condition is added that reflects the physical security specification listed within Section 4 of this report.



Bradley Hart MTCP

Design for Security Consultant

Contents

1	Visual Audit.....	4
2	Crime Statistics & Analysis.....	5
	2.1 Crime Summary	
	2.2 Non-Domestic Burglary (Manchester Industrial): Risk Analysis	
	2.3 Theft (Manchester Industrial): Risk Analysis	
	2.4 Non-Domestic Burglary (Manchester Offices): Risk Analysis	
	2.5 Theft (Manchester Offices): Risk Analysis	
	2.6 Local Vehicle Crime: Risk Analysis	
	2.7 General Risk Factors	
	2.8 Common Use-Specific M.O.s (Modus Operandi)	
3	Layout Appraisal.....	11
	3.1 Proposed Development	
	3.2 Positive Aspects of the Proposal	
	3.3 Points for Further Consideration	
4	Physical Security	13
	4.1 Doors	
	4.2 Windows & Shutters	
	4.3 Glazing & Building Fabric	
	4.4 Access Controls	
	4.5 Alarm	
	4.6 Boundaries	
	4.7 Car Park	
	4.8 Lighting	
	4.9 CCTV	
	4.10 Landscaping	
	4.11 Other	
5	Management & Maintenance	18
6	Construction	18
7	Useful References	18
	7.1 Secured by Design (SBD)	

Appendix

A	Contact Register.....	19
B	Associated Documents.....	19
C	CIS Version History	19
D	Glossary	20

1 Visual Audit

The site lies within the new Airport City South area adjacent to Manchester Airport – a World Logistics Hub due to be completed in phases over the next 10 to 15 years. Airport City South lies between the M56 motorway to the west and the A538 Wilmslow Road to the east.

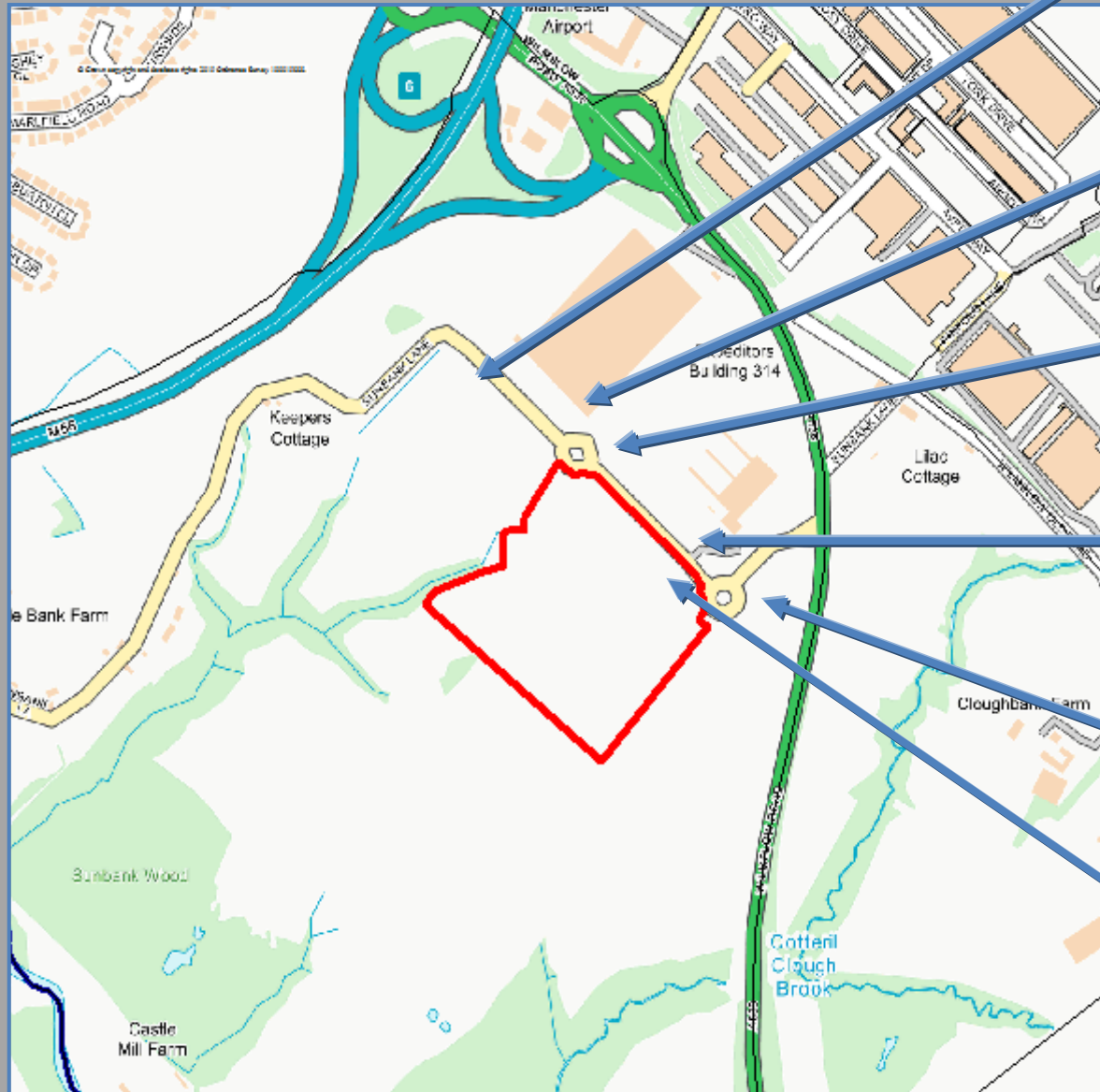
The site itself lies on the south-west side of Sunbank Lane, opposite the existing DHL site and a number of recently constructed commercial units fronting to the north-west. It currently formed by relatively open grassland and some scrub vegetation.

The land to the north and east of the site (between Sunbank Lane and Wilmslow Road) has already been developed, including DHL and Amazon distribution warehouses and a block of commercial units. To the north-east of the site, also accessed off Sunbank Lane, is a BP petrol station with an M&S Food retail unit and a Costa drive-through coffee shop.

The plots to the east and west of the development site are also due to be developed to provide large scale industrial/distribution warehouses (with ancillary offices) and work has recently begun on the site to the west.

Given that Airport City South is currently in its infancy (with the majority of its Plots still to be developed) and the adjacent land to the west, east and south is currently formed by open pasture/grassland (including belts of Woodland around the Bollin Valley), as well as streams and some public rights of way.

As such, the area surrounding the site currently benefits from limited levels of activity, overlooking and natural surveillance - particularly at night, which is also when industrial/commercial sites are typically closed or operate with reduced staff numbers. Such open land/secluded routes can provide opportunities for crime with a low risk of detection, by providing easy access/escape routes for offenders to utilise unseen when targeting nearby buildings or sites.



2 Crime Statistics & Analysis

All data below is based on crimes recorded between 1st June 2018 to 31st May 2019.

2.1 Crime Summary

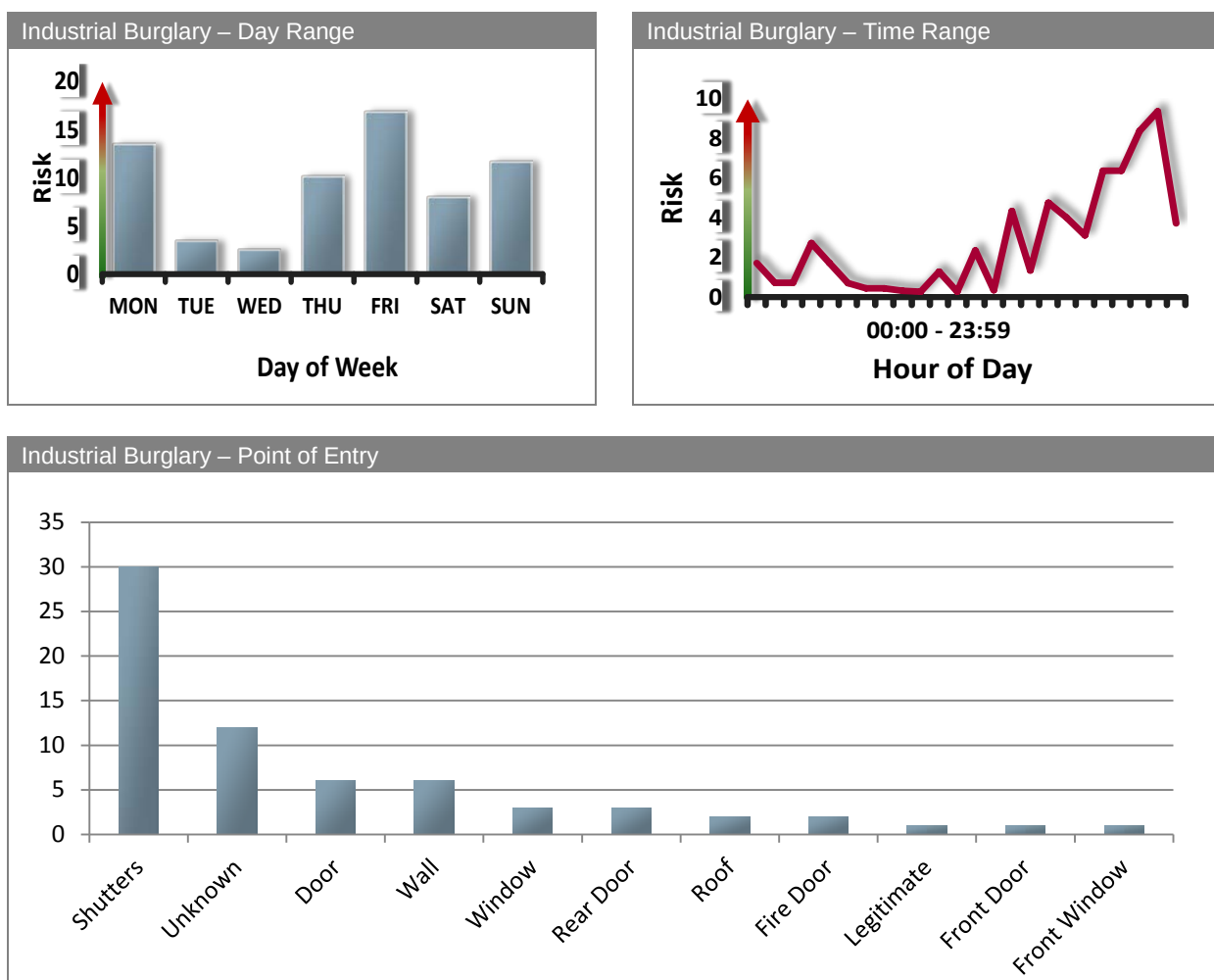
Figure 1: Recorded Crime within 500m of Site

Domestic Burglary	Non-Domestic Burglary	Criminal Damage	Less Serious Wounding	Theft	Robbery	Serious Wounding	Theft from Motor Vehicle	Theft of Motor Vehicle	Bicycle Theft
<5	<5	<5	<5	6	<5	<5	6	<5	<5

- 2.1.1 Over the last 12 months, the general volume of crime in the local area has been very low. This can be largely attributed to the presence of large areas of open space and transport infrastructure in the surrounding area, resulting in a low density of developed land that attracts few crime and disorder incidents.
- 2.1.2 As this Crime Impact Statement relates to a proposed industrial unit with ancillary offices, more detailed analysis below will look at use-specific burglary and theft.

2.2 Non-Domestic Burglary (Manchester Industrial): Risk Analysis

The data below relates to non-domestic burglary offences within/against industrial units, recorded in the Manchester area.



- 2.2.1 **Day Range:** During the week, the risk of burglary at Manchester industrial premises peaks on Friday and is lowest on Tuesday and Wednesday.

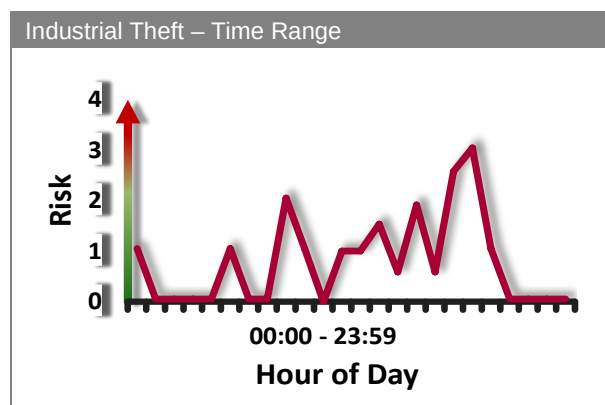
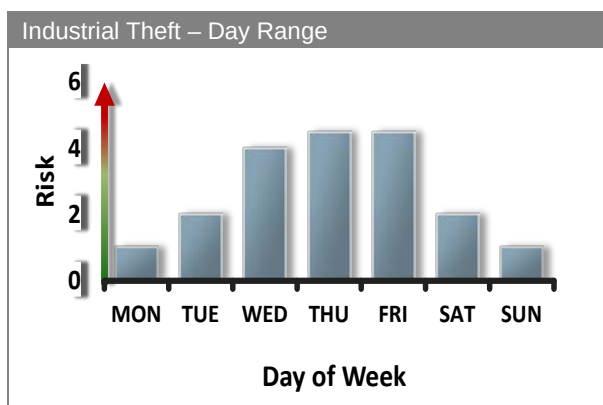
2.2.2 **Time Range:** The risk of burglary rises from late afternoon, peaking late at night. Offenders often target industrial premises at these times when it is dark, industrial areas are typically quiet, units are often closed or operate with fewer staff and offenders perceive a lower risk of being observed or detected.

2.2.3 **Point of Entry:** When targeting Manchester industrial premises, the following entry points have been utilised most frequently:

- Offenders have damaged or forced shutters upwards to gain unauthorised access or to gain access to doors and windows behind them.
- In a number of cases, the point of entry was 'unknown'. This is likely to have been where offenders have posed as legitimate customers, visitors or employees before gaining access to back-of-house/staff areas and stealing property unnoticed.
- Doors have been forced open using tools/implements or when they have been left insecure by members of staff.
- Offenders have penetrated through the walls of industrial units, using vehicles or tools, to gain access.
- Glazing within doors and windows has been smashed to gain entry.

2.3 Theft (Manchester Industrial): Risk Analysis

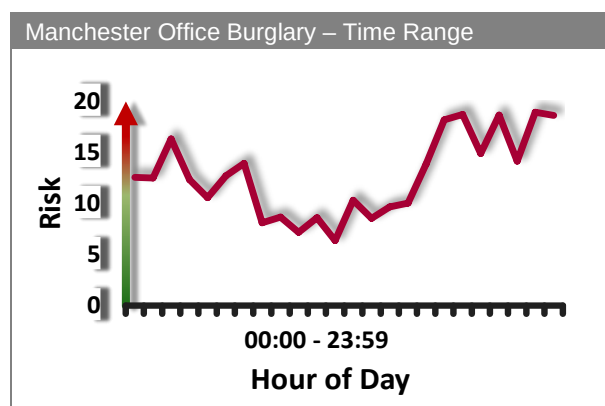
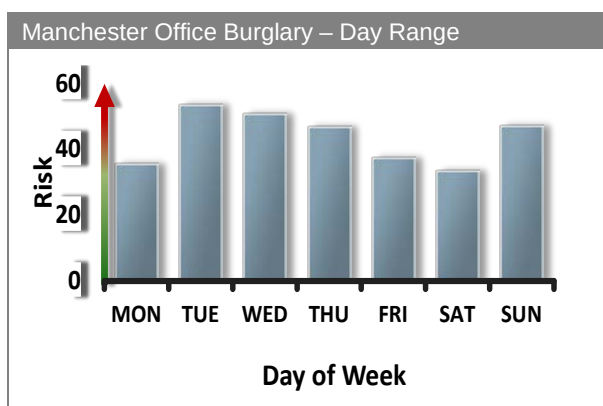
The data below relates to thefts within/against industrial units, recorded in the Manchester area.



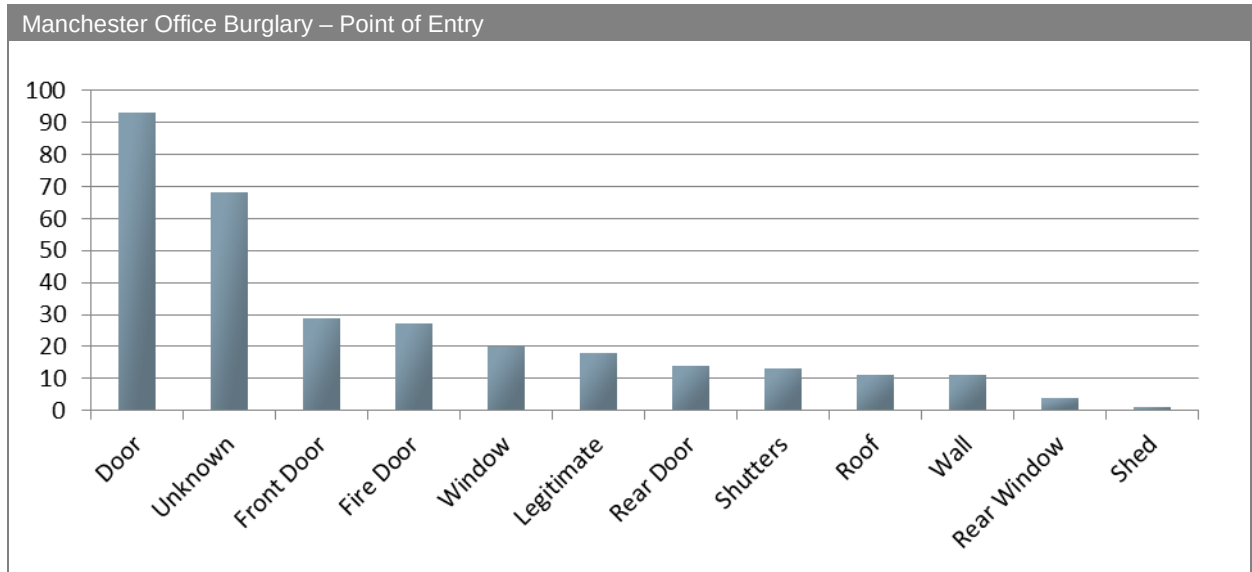
2.3.1 **Day & Time Range:** The greatest risk of theft at Manchester industrial premises is experienced mid-week (i.e. Wednesday to Friday). During the day, the risk peaks during the afternoon and into the early evening. There are two common occurrences of theft – the theft of personal property from within buildings (e.g. cash, bags, wallets/purses etc.) and the theft of tools, materials and plant stolen from service/storage yards.

2.4 Non-Domestic Burglary (Manchester Offices): Risk Analysis

The data below relates to non-domestic burglary offences within/against office premises, recorded in the Manchester area.



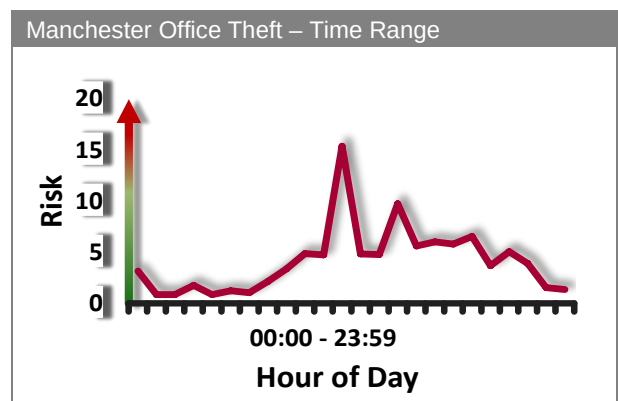
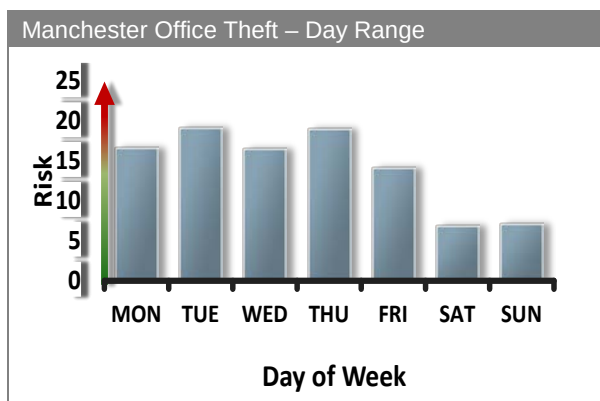
- 2.4.1 **Day Range:** During the week, the risk of burglary at office premises in Manchester peaks on Tuesday.
- 2.4.2 **Time Range:** During the day, the risk of burglary rises at night/into the early hours of the morning. Such premises are often targeted at these times when they are closed and unoccupied, meaning offenders can attempt to gain unauthorised access without fear of being disturbed or identified.



- 2.4.3 **Point of Entry:** When targeting Manchester offices, the following entry points have been utilised most frequently:
- Secure doors have been forced open using body pressure, implements and tools. Many burglaries against Manchester office buildings do not appear to be opportunistic, with offenders often bringing equipment with them that can be used to force open doors and cut locks.
 - A large proportion of burglaries have been committed through 'unknown' points of entry, which are likely to have been where offenders (posing as legitimate customers, visitors or employees) have gained unauthorised access to staff only areas (i.e. through insecure doors, tailgating etc.) to steal property.
 - Glazing within windows and doors has been smashed to gain unauthorised access.
 - Shutters have been prised open to target doors/windows behind them.

2.5 Theft (Manchester Offices): Risk Analysis

The data below relates to thefts within/against office premises, recorded in the Manchester area.

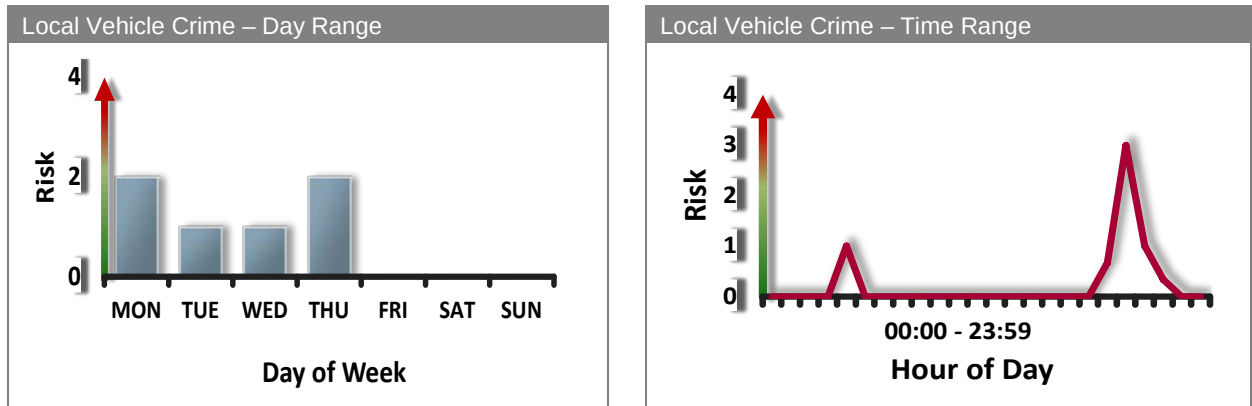


- 2.5.1 **Day Range:** During the week, the risk of theft at Manchester offices is greatest during the working week, when the opportunities to offend are greater, and is significantly lower at the weekend, when many offices premises are closed or operate on reduced opening hours/staffing levels.

- 2.5.2 **Time Range:** During the day, the risk of theft is concentrated during normal working hours – peaking around midday. During these times, many office workers will take their lunch breaks, leaving unattended property at desks or in insecure areas. Thefts can also often happen at the end of the working day, when members of staff are finishing work and premises is likely to be less secure, such as while cleaning operations are carried out. Purses/wallets, cash, mobile phones and other items of technology (such as laptops) were the most frequently stolen items.

2.6 Local Vehicle Crime: Risk Analysis

The data below relates to vehicle crime committed within 500m of the site.



- 2.6.1 **Day/Time Range:** Over the last 12 months, there have been relatively few recorded vehicle crimes in local area surrounding the site. Those that have occurred have taken place to the east of the site and during the evening – when it is dark, streets are quiet and offenders perceive a lower risk of being witnessed. Vehicles parked within open car parks for long periods of time have been targeted most frequently, where they are easily accessible and cannot be easily overlooked by their owners.

2.7 General Risk Factors

- 2.7.1 The typical security risks for a development of this nature are:

- Burglary
- Robbery to business
- Violence towards staff
- Theft of personal belongings at work
- Criminal damage to property and vehicles
- Unauthorised access to buildings/private space
- Arson
- Cycle theft
- Employee theft
- Theft of/from parked vehicles
- Theft and criminal damage during the construction period

2.8 Common Use-Specific M.O.s (Modus Operandi)

2.8.1 Having looked at the crime data for the site/surrounding area and the proposed land uses, the most frequent M.O's (modus operandi) used by offenders when targeting industrial/office premises are listed below, along with suggested measures to reduce the risk of them being utilised at the proposed development:

- **Manchester Industrial & Offices:** Shutters have been forced upwards to gain unauthorised access or to access doors/windows behind them

Possible Solution - Roller shutters can appear secure in that they are difficult to penetrate, however physical security products are only as strong as their weakest component. A security-certified shutter (see Sections 4.1/4.2) has an independently proven level of resistance, and ensures that all aspects of the shutter (locks, rails, laths etc.) have been scrutinised by professionals. If external shutters are used, the shutter boxes and guides should be built into the fabric of the building to deter tampering/attack. Avoid locating shutters in concealed areas where a concerted attack from an offender is unlikely to be witnessed. Ensure that parked vehicles and stored materials do not obscure sight lines.

- **Manchester Industrial & Offices:** Offenders posing as legitimate customers, visitors or employees have gained unauthorised access to staff only areas to steal property

Possible Solution – There should be a robust access control system in place to ensure that callers to the building are vetted and/or met and escorted before being allowed access into them (see Sections 4.1/4.4). All individual rooms should be capable of being secured when unoccupied and there should be secure areas for staff to store their belongings while at work. All staff should understand and accept the need for security measures and should be trained to be vigilant and to report any suspicious behaviour.

- **Manchester Industrial & Offices:** Doors have been forced open using tools/implements or when they have been left insecure by members of staff.

Possible Solution - Although the location of doors should be considered (ideally placed where they can be readily observed, so that potential criminals would be more easily detected), it is inevitable that some will be located where they will benefit from lower levels of natural surveillance. All external doors should be certified to recognised security standards (see Section 4.1), which are independently proven to reduce the risk of forced entry and thus increase the chances of detection. Security-certified doors are the best long-term measure to address this risk and can be obtained to suit virtually all operational requirements. Good use of perimeter boundaries, lighting and CCTV (see Sections 4.6, 4.8 & 4.9) can also deter criminals by preventing access to vulnerable areas and increasing the chances of them being seen by security personnel or passers-by.

- **Manchester Industrial & Offices:** Glazing within windows and doors has been smashed to gain unauthorised access

Possible Solution – All ground floor/accessible glazing (including in and around doors) should include a laminated pane (see Section 4.3), which forms a much more robust barrier against shattering and penetration. The strength of the laminated glass should be relative to the strength of the door or window system in which it is fitted. Where possible, the size of any glazed elements within/directly adjacent to doors should be reduced and set well away from locking points.

- **Manchester Industrial:** Offenders have penetrated through the walls of industrial units, using vehicles or tools, to gain access

Possible Solution - There should be a block work wall or material of similar strength (see Section 4.3) behind or within any cladding to buildings, to a minimum height of 2000mm from ground level, to ensure that the building fabric itself is not vulnerable to attack. Boundary treatments, lockable gates, vehicle barriers or bollards should also be incorporated to prevent unauthorised vehicles from getting close to the buildings out-of-hours (see Section 4.6).

-
- **Manchester Industrial:** Theft of externally stored materials, tools and plant equipment

Possible Solution - The integrity of the boundary treatments should be evaluated and regularly checked for defects. Inappropriately parked vehicles/trailers and other externally stored items can obscure the spread of lighting and CCTV coverage, creating potential areas of intense shadowing and blind spots. It is recommended that this is considered in the external arrangement, and 'no store/park' areas specifically identified to avoid inadvertently blocking surveillance. Storage/parking areas close to boundaries should also be avoided as they may mask any damage to perimeter fencing.

3 Layout Appraisal

3.1 Proposed Development

- 3.1.1 The proposal is to develop the site for industrial purposes, with two alternative schemes proposed:
- 3.1.2 **Option 1** – A 49,192sqm. single-sided unit comprising of 3 storey offices to the north-east corner of the building, a two-storey hub office within the service yard to the north-west of the building and a large industrial warehouse. A 382 no. space car park is proposed along the south-eastern façade of the building and a large, enclosed service yard is proposed to the north-west, comprising of 40 no. docks (including 8 no. euro docks).
- 3.1.3 **Option 2** – A 36,975sqm. cross dock unit comprising of 3 storey offices to the north-east corner of the building, 2 no. two-storey hub office within the service yards on each side of the building and a large industrial warehouse. A 330 no. space car park is proposed along the street frontage (north-east) of the building, with large service yards to both the north-west and south-east sides of the building, each comprising of 20 no. docks (including 4 no. euro docks)

3.2 Positive Aspects of the Proposal

The following proposed features would make a positive contribution to the prevention of crime and fear of crime.

- 3.2.1 The proposed development will bring a vacant site into use and provide additional activity and surveillance to the area.
- 3.2.2 The site sits within an established and developing commercial estate, within which some units operate on a 24 hour basis, providing some legitimate activity/overlooking and passive surveillance to the area at all times of the day and night.
- 3.2.3 The layout of the building within each option is relatively simple, with no recesses that could provide cover for covert criminal activity. The external façade of the building should provide little opportunity to scale the structure.
- 3.2.4 Each option will feature service yards enclosed with a security fenceline, with gates/barriers to control legitimate access and prevent unauthorised access. The car parks will be located where they can be at least be overlooked from the street or from the windows of the proposed offices.
- 3.2.5 The principle entrances to the buildings within each option will be in a prominent positions, where it will be capable of being clearly seen from the street.
- 3.2.6 The proposed development provides the opportunity to include security features built into the design and construction of the building and avoid the need for obtrusive retro-fitted security measures that can increase the fear of crime. Security measures carefully incorporated into the design can ensure the units are reasonably secure, without visibly announcing that the design was concerned about crime.

3.3 Points for Further Consideration

The following points have been identified for further consideration and would need to be addressed for Design for Security to support the proposed scheme.

- 3.3.1 The site currently abuts publicly accessible open land to the north-west, south-east and south-west (as well as potentially diverted public rights of way), which benefits from little/no overlooking or natural surveillance. This could leave exposed perimeter fencing or the fabric of the building itself (if left open/accessible) potentially vulnerable to damage and unauthorised access, as offenders could access them unseen and operate for a long period of time without fear of being detected. In addition to securely enclosed service areas (see Section 4.6), it is therefore highly recommended that all exposed and potentially vulnerable facades of the building are enclosed within a secure fenceline in order to provide another layer of security to the building shell. Ideally, the whole site should be securely enclosed, including the car park and the street frontage of the building. If left accessible, the car park could be vulnerable to being mis-used out-of-hours (e.g. by joyriders, by travellers or by passengers using the airport etc.) and the fabric of the building could also be vulnerable if unauthorised vehicles could get close to it when closed. If the whole site cannot be fully enclosed within a secure fenceline, consideration should at least be given to protecting the street frontage of the building with anti-ram

bollards (or similar hard/soft landscaping features) and enclosing the car park with bollards, low-level railings or steel knee-rails and vehicles arm barriers to prevent unauthorised access and allow it to be secured out-of-hours (again, see Section 4.6 for more information).

- 3.3.2 The control of access into and around the building itself is also paramount to it's security. There should be a reception desk within the entrance lobby (staffed at all times when the building is operational), which should have full surveillance of everyone entering/leaving the building. All visitors should report to reception for vetting by staff before gaining access to the rest of the building. The main entrance doors should be capable of being controlled remotely by reception staff if required to prevent unauthorised access. All individual offices, plant areas or rooms housing sensitive/desirable items should be capable of being secured when unoccupied (see Sections 4.1/4.4). There should also be a secure area for staff to store their personal belongings while at work.
- 3.3.3 It is essential that all of the physical security measures listed below are incorporated into the scheme. Integrated, risk-commensurate security measures aim to place secure physical barriers or surveillance in the path of the criminal – making crime harder to commit and raising the risk of detection and possible capture, as well as promoting a feeling of safety in users.

4 Physical Security

The following checklist forms the physical security requirements for this scheme to achieve Secured by Design accreditation.

4.1 Doors

- ☐ All external doors (single and double leaf) must be compliant with and certified to BS PAS 24, STS 202, or LPS 1175 SR2. It is crucial that the door ironmongery to any escape-only doors is permitted under the security certification of the product. All escape-only doors should be alarmed (audible upon opening) and designed without visible external ironmongery.
- ☐ Access through the main entrance should be capable of being controlled remotely by reception staff, to ensure any visitors are vetted or are greeted/escorted before being allowed access into the building (see Section 4.4 for more information).
- ☐ If the main external entrance to the offices is to be formed by a revolving doorset, it will not be capable of achieving the above standards. Revolving doors should be tested and certified to BS ENV 1627 (WK2+). If circumstances could prevent this, please consult with Design for Security. Outside of normal working hours or if the building is to be open at any time without reception staff within the lobby area, the revolving door should be secured and an adjacent single-leaf entrance door (which should be compliant with and certified to BS PAS 24 or LPS 1175 SR2) should be utilised and controlled by staff key-fob/card or by means of a video access control system linked to a central security office, allowing staff to vet visitors before allowing them access (again, see Section 4.4 for more information).
- ☐ Any sectional loading bay doors must be tested and certified to LPS 1175 SR2. If circumstances could prevent this, please consult with Design for Security.
- ☐ The doors/frames to internal offices, meeting rooms, back-of-house plant/service/stores etc. should be robust/solid-core (minimum 44mm thick) and capable of being secured when unoccupied. Staff should be able to store their belongings in a secure area while at work.

4.2 Windows & Shutters

- ☐ All windows, where possible, should be certificated to BS PAS 24. All other window designs/dimensions should take account of the requirements of the above standards, as certified products can carry dimensional restrictions. Any curtain walling panels should include laminated glazing (see below) and should ideally be securely fixed directly to the floor slabs where possible, rather than to perimeter columns.
- ☐ All ground floor and any other easily accessible opening lights (escape requirements permitting) must be lockable and have fixed/lockable opening restrictors (not releasable from the outside) limited to 100mm.
- ☐ If shutters are to be installed, they should be tested and certified to LPS 1175 SR2 (or SR1 if perforated laths are required) and installed in accordance with manufacturer's instructions. Ideally, shutters should have shutter-boxes and guides built into the fabric of the building – where they would be less vulnerable to attack and less visually intrusive.

4.3 Glazing & Building Fabric

- ☐ Glazing to a height of 2400mm (or if otherwise accessible) must incorporate at least one pane of glass with a 1.5mm PVB interlayer (e.g. 7.5mm laminated glass), or a glass rated as P4A under EN 356. The remaining pane in a double glazed unit may be toughened glass.
- ☐ There should be a block work wall or material of similar strength (e.g. welded-steel mesh) behind or within any cladding to the building, to a minimum height of 2000mm from ground level, to ensure that the building fabric itself is not vulnerable to attack.

- ☐ Any louvres to plant areas should be robustly constructed and fixed, to ensure they cannot be easily removed, and designed to ensure that they cannot be used as a climbing aid to reach upper floor windows. Security-certified louvered doorsets are also available if required (search SBD compliant products at <https://www.securedbydesign.com/member-companies/accredited-product-search>).

4.4 Access Controls

- ☐ Access control systems should be operable by swipe card or fob, and not numeric key pads. The following doors/gates should operate on access control:
 - The main entrance door/s if/when required by reception staff, outside of normal working hours or when reception is not staffed.
 - Consideration could also be given to turnstile/barriers within the entrance lobby controlling access to the lift/stair cores, operated by reception staff or by staff fob/card.
 - Any staff-only external entrance doors providing access to/from parking areas or service yards.
 - Vehicular and pedestrian entrance barriers/gates to the service yards.
 - Any internal doors providing access to obvious high risk areas (e.g. server rooms, storage areas etc.)
 - Doors to any staff changing facilities/lockers and cycle stores.
- ☐ The electric locking system to be used throughout the building should be fully auditable (i.e. allowing the retention of data, such as who accessed where and when), to allow for a better investigation into any incidents. Staff cards/fobs should be capable of being easily and quickly activated/disabled to ensure that mis-use is prevented. Staff should only be allowed access to areas required for their work and keys/passes should only be carried if required for duties and should be accounted for at all times.

4.5 Alarm

- ☐ A monitored alarm system should be installed, linked to contacts on all external doors/shutters and PIR detectors covering all ground floor areas with windows, with a signal terminating at a recognized Alarm Receiving Centre (ARC) or security control room.

4.6 Boundaries

- ☐ The service yard enclosure/s, as well as the south-western (rear) façade of the building, should be enclosed with 2400-3000mm high-security, rigid-panel, welded-wire mesh fencing (ideally 358 gauge, with small apertures to deter scaling and cutting) with anti-tamper fixings to secure the panels to posts (please see <https://www.securedbydesign.com/member-companies/accredited-product-search> for a list of Police approved perimeter security suppliers). The access and egress gates to service yards should be controlled via an audio/visual access-control system linked to a staffed security office or should be operated from an immediately adjacent staffed gatehouse. Sliding gates are preferred, but if double gates are used they should overlap when closed and should not be capable of being forced open. Any pedestrian gates should be should also be 2400-3000mm high, self-closing/locking and operated by staff key-fob on access and egress. Exposed hinges and large sliding bolt apertures/locking points to any gates should be avoided, or fitted with shrouding/protective plates (see opposite) to avoid the creation of footholds. If panic mechanisms are required on the inner face of pedestrian gates, they should not be capable of being reached/operated from the external face of the fence/gate.



-
- ☐ Ideally, the car park to the south-east of the building within Option 1 and the car park to the north-east of the building within Option 2 should be enclosed within a secure perimeter enclosure (as described above), to allow them to be secured outside of normal working hours/when closed. At the very least, the parking areas should be enclosed with bollards (or similar hard/soft landscaping features), low-level railings or steel knee-rails. Vehicle arm barrier (operated by staff key-fob/card or remotely by reception staff) should also be provided to the vehicular entrances of the car parks to prevent unauthorised access and allow them to be secured out-of-hours.
 - ☐ Care should also be taken to ensure there are no trees or any other hard/soft landscaping features immediately adjacent and on the publicly accessible side of any secure boundaries that could be used as a climbing aid to scale the fencing. Any such features should be pruned or removed where possible. The site boundary treatment should also be positioned on hard standing ground. Where this is not possible, the ground conditions should be reviewed as extra measures may be required to create a secure boundary.
 - ☐ It is highly recommended that condition of the fencing along the perimeter of the site is regularly inspected for signs of damage/attack and is repaired immediately if any incidents are experienced. Where exposed, the perimeter fencing to the service yards should be protected on the inner side from potential damage from large vehicles, using crash barriers or rails, to deflect any encroachment and maintain a secure boundary.

4.7 Car Park

- ☐ Lighting to all parking areas should be in accordance with BS 5489, with an average lux level 20 and a uniformity level of no less than 25%.
- ☐ The surface of the car park should be even tarmac. The integrity of the surface treatment should be maintained to ensure that there is no loose material that can be used to commit crime.
- ☐ Bays and directional markings should be clearly demarcated to avoid confusion or conflict, with pedestrian routes/directions clearly signed.
- ☐ Where feasible, a one-way system should be implemented to reduce the likelihood of collisions and conflicts. Traffic calming measures should be incorporated to limit the speed of vehicles within the site.

4.8 Lighting

- ☐ External lighting must be provided to all access roads, parking areas and service yards within the site, in accordance with BS 5489.
- ☐ Fittings should produce 'white' light, as opposed to yellow/orange light. Metal halide (or bulbs with a comparable output) should be used, as these offer superior colour rendition over alternatives such as high and low pressure sodium bulbs.
- ☐ Dusk 'til dawn lights, operated by photoelectric cell/daylight sensor, should be installed to all external doors.
- ☐ Lighting fixtures must not be positioned to provide climbing aids over boundary treatments. Electrical and architectural layouts should be developed together to avoid this.

4.9 CCTV

Any CCTV system that may be used within this proposal will require certain specifications and intelligent placement of cameras to compliment the design of the development. Designers should consider the following points when planning a CCTV strategy:

- ☐ CCTV systems (and lighting that support them) require regular cleaning and maintenance to remain effective.
- ☐ Where necessary cameras that are vulnerable to damage should be protected from attack either by relocation to a higher level and using a bigger lens to achieve the view required or through the fitting of a vandal resistant housing.
- ☐ With regards to the retention of footage, the police prefer quality over quantity. The overall retention period should be dictated by what the system is designed to achieve, though it would be better to have good quality images over a 14-day period than poor ones over a 30-day period.
- ☐ Procedures for recovery of recordings are recommended to be established (e.g. trained staff / the CCTV system instruction manual to be readily available). This is to ensure that the images produced will be of an [acceptable standard](#) that will allow for [identification](#) of an individual which will stand up to scrutiny in court.

Acceptable Standard - this generally requires a resolution of 720x576 pixels at a real time frame rate of 25 frames per second. (N.B. Both the camera and DVR must be capable of this – if the camera will only send low resolution images then it does not matter how high the resolution of the recording unit is).

Identification – One of three levels of field of view. To identify an individual, the image must capture no less than 120% of the field of view (at least from the top of the individuals head to their knees). The remaining two levels of field of view are 'Overview' and '[Recognition](#)', which whilst effective for observational purposes, are less likely to result in the identification of a person/offender.

- ☐ The intelligent placement of cameras helps to provide clear facial identification of individuals. Suitable locations would be: [the entrance/s to the site](#), [the main entrance lobby to the building](#), [all external elevations](#) and [all service/parking areas](#).

4.10 Landscaping

- ☐ In vulnerable locations such as around site/building entrances, parking areas and footpaths, low planting should not exceed 1000mm in height and tree canopies should fall no lower than 2000mm from the ground. This is in order to allow unimpeded surveillance and eliminate hiding places. A maintenance agreement should stipulate that these planting dimensions would be adhered to.
- ☐ Loose surface materials in the publicly accessible areas of the scheme should be avoided. Small fragments of ground covering can be used as missiles against people and premises (both to gain entry and to commit criminal damage).
- ☐ Planting must be avoided that will aid climbing over boundary treatments. The security of fences can be compromised if trees or street furniture are placed close by.

4.11 Other

- ☐ The position of ancillary structures, parked trailers and any external storage areas should be carefully considered in relation to the following:
 - Their potential to block sight lines and create hiding places.
 - Their potential to obscure CCTV and lighting.
 - Their potential to create climbing aids that would assist unauthorised exit/entry over boundary fencing.
 - Their potential to obscure damage to fencelines.

Any proposed lighting columns, street furniture, tree/shrub planting etc. within or external to the site perimeter should also be reviewed in relation to the above issues.

- ☐ Any external cycle parking areas should be located where they can be well-overlooked from within the building and should include 'Sheffield' type stands, which both wheels and the crossbar can be locked to rather than just the crossbar (wheel slots and butterfly racks are not suitable). For further information, please refer to our cycle storage guidance document: <http://designforsecurity.org/all-downloads/>.
- ☐ Any external bin/recycling stores should be a secure, lockable and fire resistant enclosure. A strategy should be defined to ensure waste collection can take place whilst retaining a secure development.
- ☐ Any lockers within staff changing facilities must be robust/secure and all users should be encouraged to use them and not leave belongs unattended in changing areas. Staff should undertake regular inspections of any changing facilities and locker areas.

5 Management & Maintenance

- 5.1.1 There should be a comprehensive security regime in place for the day-to-day running of the site. There should be regular reviews/exercises to ensure that it remains accurate, workable and up-to-date. All staff should understand and accept the need for security measures and it should be made easy for people to raise concerns or report observations.
- 5.1.2 The upkeep of a development over its lifetime can be crucial to the level of security and safety within. Aspects of a development, which are left to deteriorate, have the potential to attract further crime – a process known as ‘the broken window theory’. A maintenance plan should be drawn up to address issues such as:
- Repair to communal areas (lighting, signage, access controls, CCTV etc.)
 - A weekly physical check of all perimeter fencing to check for evidence of breaches
 - Trimming and pruning to shrubs and trees
- 5.1.3 All high value equipment (e.g. computers, tools, plant/equipment etc.) should be property marked and securely fixed or stored to deter damage/theft. An accurate record should be maintained which logs all such items.
- 5.1.4 Adequate signage should be deployed in all areas not only to direct people throughout the site and the building, but also to deter unauthorised access to restricted areas.

6 Construction

- 6.1.1 Untidy sites and their surroundings can be littered with debris accessible to vandals who often use loose materials as missiles to commit crime. The client should take measures appropriate to secure their site during construction, and control pedestrian and vehicular access in to and out of the site curtilage. It is also recommended that the contractor on this scheme is a member of the ‘Considerate Constructors Scheme’, who has committed to be a considerate and good neighbour, as well as clean, respectful, safe, environmentally conscious, responsible and accountable.
- 6.1.2 Site security contractors should be SIA (Security Industry Authority) approved to ensure professional standards are adhered to (please see <http://www.sia.homeoffice.gov.uk/pages/acs-intro.aspx> for more details).

7 Useful References

7.1 Secured by Design (SBD)

- 7.1.1 Secured by Design focuses on crime prevention at the design, layout and construction stages of homes and commercial premises and promotes the use of security standards for a wide range of applications and products. To apply for Secured by Design certification for your development, visit our online application form at: <http://www.designforsecurity.org/secured-by-design/sbd-accreditation/>

A Contact Register

Date	Contact With	Summary of Contact
10 th June 2019	Stoford	Receipt of CIS application form & option site plans.
13 th June 2019	Stoford	Confirmation of instruction & fee
20 th June 2019	GMP Finance Dept.	Confirmation of payment

B Associated Documents

This report is based on the following drawings and supplementary information submitted by the applicant.

Drawing No.	Drawing Title	Date	Rev
SK-03-06-19-01	Site Layout Plan (Cross Dock Option)	June 19	-
SK-03-06-19-02	Site Layout Plan (Single Sided Unit)	June 19	-

PLEASE NOTE - In the event of any subsequent material changes to the scheme, it will be necessary for Design for Security to reassess the comments made within this report.

C CIS Version History

Version	Revisions Made	Date
A		

D Glossary

Burglary Resistance Standards

BS PAS 24-1, 2016

General security performance requirements for door/window assemblies.

An attack test standard for doorsets and windows. This is the minimum police requirement for Secured by Design dwellings, and is also applicable to French/double doors, and sliding doors.

ENV 1627-30 (Security Ratings WK1 to WK6)

Windows, doors, shutters - Burglar resistance Requirements and classification

The classification system used in ENV 1627-30 is aimed at the commercial market and is based on five elements:

- a) Resistance of glazing
- b) Performance of hardware
- c) Resistance to static loading
- d) Resistance to dynamic loading
- e) Burglary resistance by manual intervention

LPS 1175 (Security Ratings 1 to 6)

Specification for testing and classifying the burglary resistance of building components

This includes doors, shutters, garage doors and grilles typically for commercial premises and higher risk domestic premises and is acceptable to the ABI and the Police. The standard has 6 levels, 6 being the highest, with levels 1 and 2 equivalent in many respects to BS PAS 24 and BS 7950.

STS 201 Issue 4: 2012

Enhanced security requirements for doorsets and door assemblies for dwellings to satisfy the requirements of PAS23 and PAS24

STS 202 Issue 3: 2011

Requirements for burglary resistance of construction products including hinged, pivoted, folding or sliding doorsets, windows, curtain walling, security grilles, garage doors and shutters.

This specifies a broadly similar range of attack tools and times to those specified at the lower levels of LPS1175.

EN 356, 2000 (Ratings P1A to P8A)

Glass in building. Security glazing. Testing and classification of resistance against manual attack.

A performance standard for manual attacks on glazing. P2A is comparable to the performance of a 6.8mm laminated glass, and P4A to that of a 9.5mm laminated glass.

Commonly Used Acronyms

CIT

Cash in transit (refers to vehicles, personnel and routines).

CPTED

Crime Prevention Through Environmental Design

CRS

Crime Reduction Specialist. Sometimes known as CPO (Crime Prevention Officer)

INPT

Integrated Neighbourhood Policing Team.

PVB/PolyVinyl Butyral (Glazing interlayer)

A commonly used interlayer used in the production of laminated glass.

LPCB (Loss Prevention Certification Board)

A brand of the BRE Global (Building Research Establishment) family. The LPCB work with insurers, Government, police, designers, manufacturers, contractors and end users to develop methods of assessing performance and reliability of security products to ensure their fitness for purpose.

UKAS (United Kingdom Accreditation Service)

The sole national accreditation body recognised by government to assess, against internationally agreed standards, organisations that provide certification, testing, inspections and calibration services.

Useful Websites

Design for Security

www.designforsecurity.org

Secured by Design

www.securedbydesign.com

RIBA Product Selector

www.ribaproductselector.com

LPCB – Red Book Live

www.redbooklive.com

Crime Reduction (Home Office)

www.crimereduction.homeoffice.gov.uk

DAC (Design Against Crime) Solution Centre

www.designagainstcrime.org

Building for Life

www.buildingforlife.org

CLG (Communities and Local Government)

www.communities.gov.uk