



CRIME IMPACT STATEMENT

GORTON ROAD, GORTON, MANCHESTER
7no. USE CLASS B2/B8 LIGHT INDUSTRIAL UNITS

Greater Manchester Police
designforsecurity

FOR: IT Recycling Group Ltd.
VERSION A: 15/04/2024
REFERENCE: 2024/0105/CIS/01

Gorton Road, Gorton, Manchester

URN: 2024/0105/CIS/01

EXECUTIVE SUMMARY

Minor security additions/improvements recommended

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.

The layout of the proposed scheme is considered acceptable, as long as the issues discussed in more detail within Section 3.3 of this report are addressed, namely:

- The whole site should be securely enclosed within a 2400mm high perimeter boundary, taking care to ensure any ground level changes or any combination of retaining walls and fencing do not inadvertently create opportunities for offenders to easily scale boundaries or fit underneath fencing panels/gates.
- Given the site will benefit from limited levels of activity and surveillance and will include numerous units and multiple users, it is recommended that the gates at the access/egress points to the estate are operated automatically on a 24/7 basis, or at least outside of normal working hours if staff access is required (manual gates are unlikely to be utilised as effectively). Secondary fencelines/gates are recommended to prevent unauthorised access to the hidden sides/rears of the units.
- Control of access into/around the units themselves.

If these issues can be addressed as described within the report and the other physical security measures are incorporated, we 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 General Risk Factors	
	2.5 Common Local/Use Specific M.O.s (Modus Operandi)	
3	Layout Appraisal.....	9
	3.1 Proposed Development	
	3.2 Positive Aspects of the Proposal	
	3.3 Points for Further Consideration	
4	Physical Security	11
	4.1 Doors	
	4.2 Windows & Shutters	
	4.3 Glazing & Building Fabric	
	4.4 Access Controls	
	4.5 Alarms	
	4.6 Boundaries	
	4.7 Parking Areas	
	4.8 Lighting	
	4.9 CCTV	
	4.10 Landscaping	
	4.11 Other	
5	Management & Maintenance	15
6	Construction	15
7	Useful References	15
	7.1 Secured by Design (SBD)	

Appendix

A	Contact Register.....	16
B	Associated Documents.....	16
C	CIS Version History	16
D	Glossary	17

1 Visual Audit

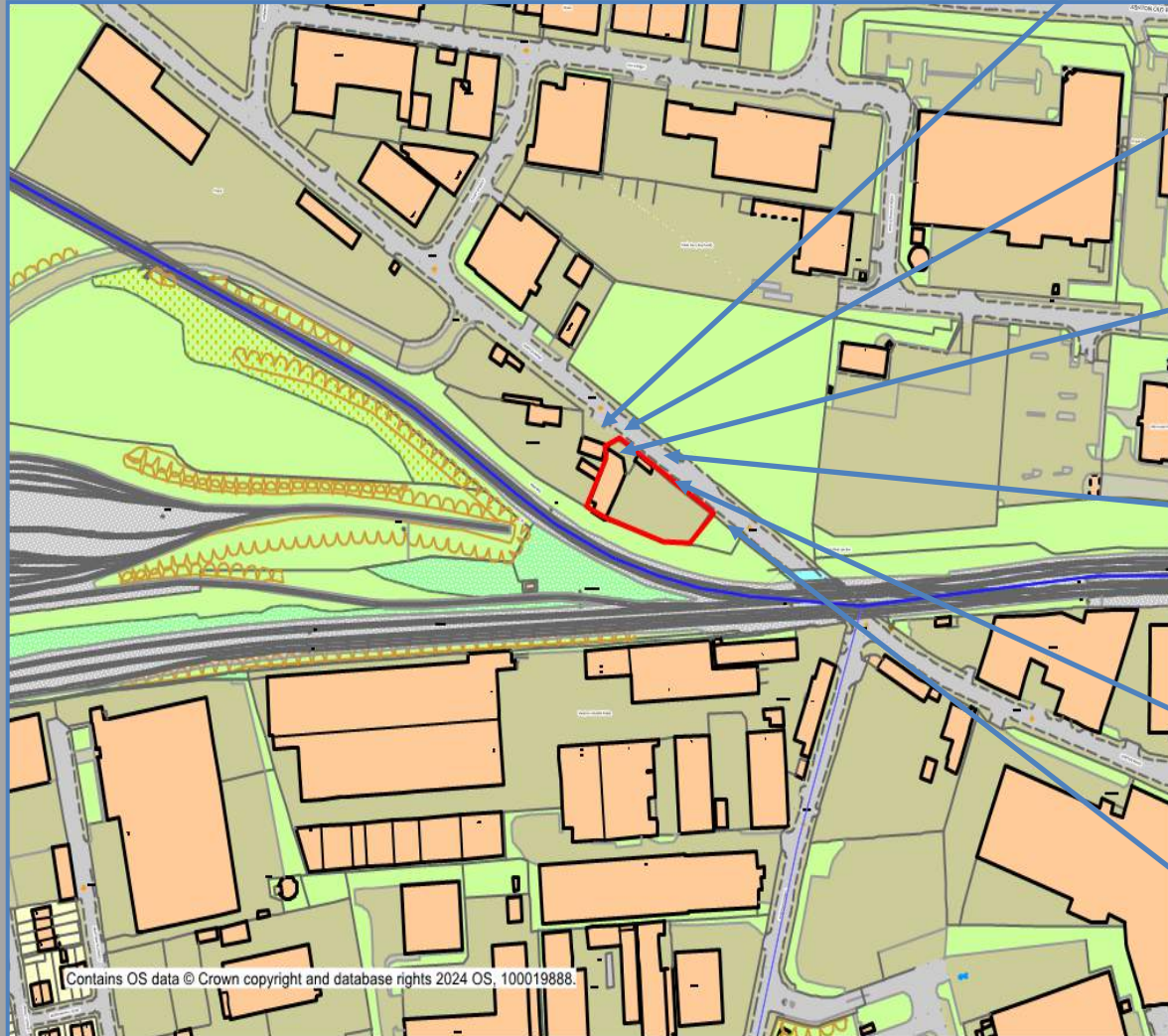
The site sits on the southern side of Gorton Road, in the Gorton area of east Manchester.

It is currently in use as a mechanical salvage yard, comprising of a series of single-storey buildings/portacabins (to the western portion of the site) and a large external storage area.

The ground level of the site sits approximately 1800mm above street level, with the street frontage formed by a high brick retaining wall with sheets of corrugated metal and scrub vegetation above. The entrance to the site (off Gorton Road) lies to the north, secured with Palisade fencing and gates. As a result of this level change, the site benefits from little/no passive surveillance from the street.

The southern and eastern boundaries of the site are formed by a 2500mm high concrete retaining wall, which separates the site from an area of vegetation beside the railway line that links Manchester Piccadilly with Hadfield and Glossop and sits at a higher ground level from the site itself. The railway line crosses Gorton Road to the south-east.

The land on the opposite side of Gorton Road from the site is vacant and also has a large brick wall along the street frontage, meaning the site is not directly overlooked. There are similar scrap yard, industrial and rail depot uses along Gorton Road to the west and east of the site – meaning it is likely to benefit from low levels of vehicular/pedestrian movement, activity and surveillance, particularly at night/when the surrounding uses are closed.



2 Crime Statistics & Analysis

2.1 Crime Summary

The crime data below is based on crimes recorded between 1st April 2023 to 31st March 2024 within 500m of the site.

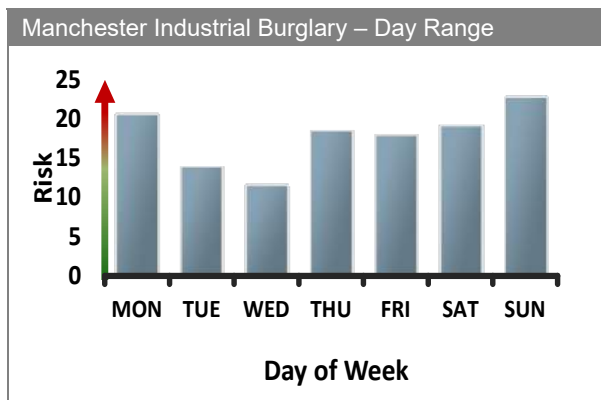
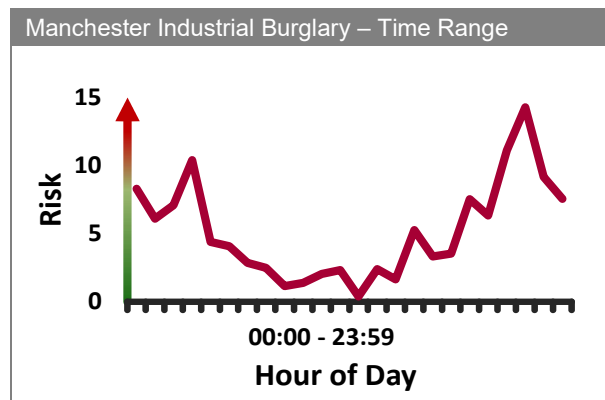
Figure 1: Recorded Crime within 500m of Site

Domestic Burglary	Non-Domestic Burglary	Criminal Damage	Less Serious Wounding	Theft	Robbery	Serious Wounding	Theft from Motor Vehicle	Theft of Motor Vehicle	Bicycle Theft
20	5	23	74	39	5	7	5	8	<5

- 2.1.1 The general volume of crime within the local area is relatively low for the Manchester division, however the area does include large areas of open space/transport infrastructure and industrial areas, which lower the density of development in the area and typically attract fewer crime and disorder incidents.
- 2.1.2 The most prevalent types of recorded crime in the local area have been less serious wounding, theft and criminal damage – with the majority of crime occurring around/off the arterial routes of Ashton Old Road (A365) to the north and Pottery Lane (A6010) to the east and the streets to the south-west (around/off Bennett Street). Less serious wounding offences have mostly involved assaults, public order offences and harassment – occurring during road rage incidents, during domestic disputes or at local educational facilities. Theft of wheel clamps and bags/mobile phones belonging to public transport users are the most prevalent types of theft in the area. Criminal damage has occurred at commercial premises, but primarily against vehicles – with offenders smashing vehicle windows, damaging bodywork and kicking/removing wing mirrors.
- 2.1.3 As this CIS relates to a proposed industrial units, the more detailed analysis below will focus on use-specific burglary and theft.

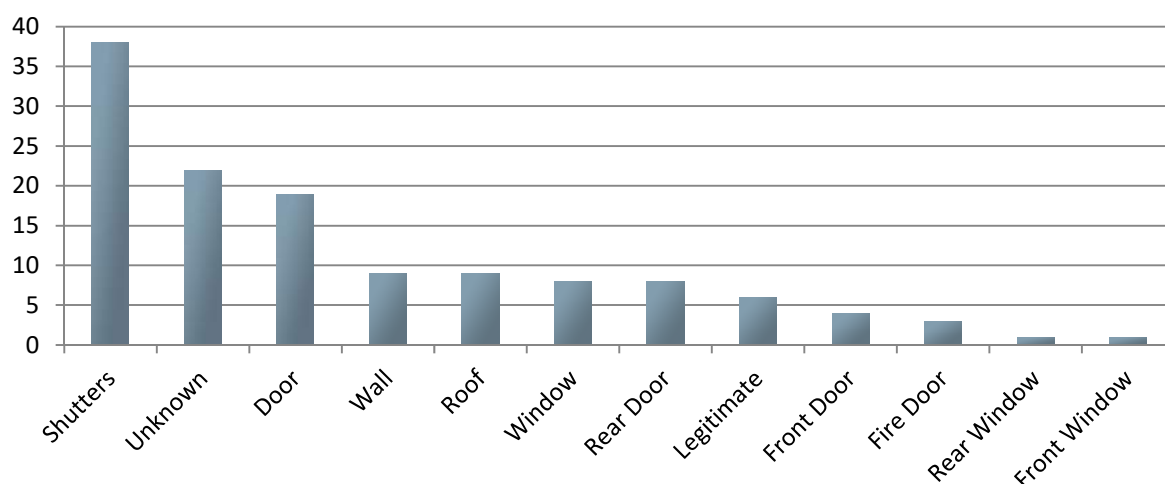
2.2 Non-Domestic Burglary (Manchester Industrial): Risk Analysis

The data below relates to non-domestic burglary offences within/against industrial units, recorded in the Manchester area 2018-2019.



- 2.2.1 **Day Range:** During the week, the risk of burglary at Manchester industrial premises peaks on Sunday/Monday.
- 2.2.2 **Time Range:** During the day, the risk peaks late at night and during the early hours of the morning. Offenders often target such commercial premises at these times when it is dark, industrial areas/streets are typically quiet, units are usually closed or operate with fewer staff and offenders perceive a lower risk of being observed or detected.

Manchester Industrial Burglary – Point of Entry



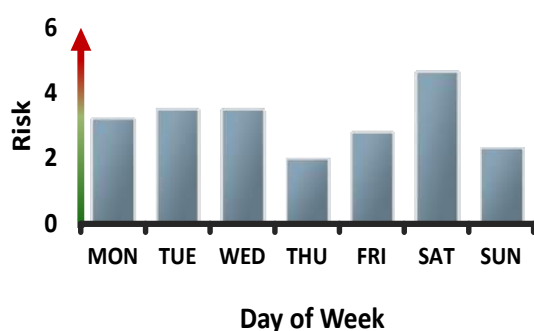
2.2.3 **Point of Entry:** At Manchester industrial premises, the following entry points and MOs have been utilised most frequently:

- Forcing open secure shutters using bodily pressure and implements (particularly metal bars and vehicles) in order to gain access.
- 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.
- Glazing within doors and windows has been smashed to gain entry.
- Offenders have penetrated through walls and roofs to gain unauthorised access.

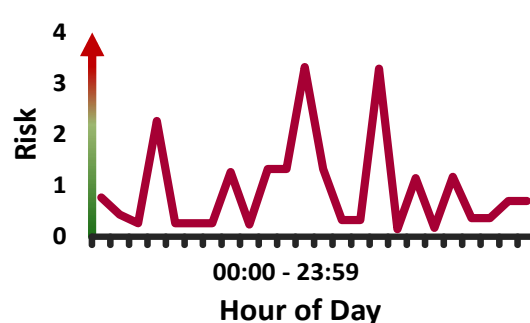
2.3 Theft (Manchester Industrial): Risk Analysis

The data below relates to thefts within/against industrial units, recorded in the Manchester area 2018-2019.

Manchester Office Theft – Day Range



Manchester Office Theft – Time Range



2.3.1 **Day Range:** During the week, the risk of theft from industrial units in Manchester peaks on Saturday.

2.3.2 **Time Range:** During the day, the risk peaks during the late morning/afternoon. There are two common occurrences of theft – the theft of personal property within buildings (e.g. cash, bags, wallets/purses etc.) and the theft of tools, materials and plant stolen from service yards.

2.4 General Risk Factors

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

- Burglary
- Robbery to business
- 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

2.5 Common Local/Use Specific M.O.s (Modus Operandi)

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

- Forcing open secure shutters using bodily pressure and implements (particularly metal bars and vehicles) in order to gain access.

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.

- 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.

Possible Solution – There should be robust access control systems in place to ensure that callers to units are vetted and/or met and escorted before being allowed access into them (see Section 4.1/4.4). All individual rooms/areas 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.

- 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.

-
- Glazing within doors and windows has been smashed to gain entry.

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. Windows that are particularly vulnerable should be secured with security-certified shutters out-of-hours (see Section 4.2).

- Offenders have penetrated through walls and roofs to gain unauthorised access.

Possible Solution - Ideally, single storey building elements should be avoided. If they are absolutely necessary, care should be taken in their design to ensure that roof areas or upper floor windows are not accessible, for example, with the use of high-level/overhanging eaves, high balustrades etc. There should be no features of the building or any nearby hard/soft landscaping features that would facilitate climbing. Any 'accessible' skylights should incorporate at least one pane of laminated glazing and should be secured with internally fixed grilles/bars to prevent unauthorised access. The construction of the roof itself and all external walls should also be robust enough to withstand penetration (see Section 4.3).

- 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 (see Section 4.11).

3 Layout Appraisal

3.1 Proposed Development

- 3.1.1 The proposal is to erect 7 no. B2/B8 industrial units, with associated site access/egress, parking and loading bays.
- 3.1.2 The existing site access will be utilised off Gorton Road, with a separate exit ramp proposed to the east of the site (also adjoining Gorton Road), allowing for one-way vehicular movement through the site. The existing brick retaining wall along Gorton Road will be retained and made-good. The existing retaining wall to the south and east boundaries will also be retained, with a terrace of two-storey units occupying the southern portion of the site. The units will front towards the one-way access road serving the site and 3 no. extended loading bays, as well as towards 10 no. vehicle parking spaces, 2 no. motorcycle spaces and cycle/bin stores. The units themselves will feature single-leaf entrance doors, roller shutter doors and first floor windows to their frontage and double fire escape doors to their rear.

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 may provide additional activity and natural surveillance/overlooking to the area when the units are operational.
- 3.2.2 Vehicular and any pedestrian access to and egress from the site will be via Gorton Road, allowing all activity, surveillance and security to be focussed in this location. The perimeter of the site will be defined by existing/proposed retaining walls and fencelines to deter unauthorised access from all directions other than access/egress points along Gorton Road.
- 3.2.3 The footprint of the buildings is simple, with no recesses that could provide cover for covert criminal activity. The buildings will also be sufficiently tall enough to make unauthorised access to the roof difficult.
- 3.2.4 The proposed car parking/servicing areas will be located directly in front of the units and will be overlooked from within the buildings themselves.
- 3.2.5 The proposed development provides the opportunity to include security features built into the design/construction of the scheme. Security measures carefully incorporated into the design/specification of the development can ensure the building is 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 whole site should be enclosed with retaining walls and high security, rigid panel, welded-wire mesh fencing/gates (please see Section 4.6 for more information) to a minimum height of 2400mm from the ground level external to the site, to ensure unauthorised access is prevented. Any combination of brick/concrete retaining walls and welded-wire mesh fencing should have fencing panels that are fixed flush with the outer skin of the retaining wall below, leaving no steps/gaps that would provide a climbing aid. Given the ground level changes surrounding the site, care must be taken to ensure that they do not inadvertently create opportunities for offenders to easily scale boundaries or fit underneath fencing panels or gates. Care should also be taken to ensure there are no trees or any other hard/soft landscaping features immediately adjacent, on the external side of the site perimeter, that could be used as a climbing aid to scale boundaries. Any such features should be pruned or removed where possible.

-
- 3.3.2 The site access and egress points along Gorton Road should be secured with 2400mm high gates to secure the site. Gorton Road has a number of high walls/inactive industrial frontages along it - meaning the levels of activity, footfall, passive surveillance and overlooking in the area are low, particularly at night/over the weekend. The retaining wall/level change between the street and the site itself also limits the levels of surveillance possible from the street. Given this, and that the site will include numerous units and multiple users (providing the opportunity for offenders to gain access to the site anonymously, without being challenged), consideration should be given to the gates at the access/egress points being operated automatically at all times, in order to prevent unauthorised access during operational hours as well as at night/when closed. The gates should be operated on access and egress by staff key fob/proximity reader or via an audio/video access control system linked to each unit – ensuring that visitors are vetted before being allowed access (see Sections 4.4 & 4.6 for more details). If the gates must be left open during operational hours, they should at least be secured and operated via access controls if staff access is required outside of normal working hours (e.g. 6pm-7am). Manual gates securing such sites with multiple tenants are unlikely to be utilised effectively. If the estate is to be open/accessible during the day, it is highly recommended that secondary fencelines/gates (which could be lower) are incorporated to prevent unauthorised access to the hidden, narrow route to the side/rear elevation of the units at all times of the day and night - see Section 4.6 for more details.
- 3.3.3 The control of access into and around the units themselves will also be paramount to their security. Ideally, entrance lobbies should be staffed at all times when the units are operational, allowing staff to have full surveillance of everyone entering/leaving the premises. All visitors should report to a reception for vetting by staff before gaining access to the rest of the unit. In the absence of a staffed reception, the main entrance doors should be capable of being controlled remotely by office or warehouse staff, to prevent unauthorised access. Any individual offices or rooms housing sensitive/desirable items should be capable of being secured when unoccupied (see Sections 4.1/4.4). If the estate is to be open/accessible during the day, it is essential that that loading bay doors to the frontages of the units are not left insecure and unattended at any time, which would allow offenders to circumnavigate the access-controlled main entrances.
- 3.3.4 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 staff/users.

4 Physical Security

In addition to the layout issues highlighted within Section 3, the following checklist forms the physical security requirements for the scheme to achieve Secured by Design accreditation.

It is recognised that if the units are being constructed on a speculative basis, some of the security measures for each of the individual units listed below (such as access-controlled entrances and intruder alarms) may be for the end owners/occupiers of the units to install rather than the developers. However, they would be required for the scheme as a whole to achieve the full SBD Award.

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. There should be no internal doors between units unless they are occupied by the same tenant. Any such doors should also be compliant with and certified to BS PAS 24, STS 202, or LPS 1175 SR2.
- ☐ Access through the main entrance of each unit should be capable of being controlled remotely by staff, to ensure any visitors are vetted or are greeted/escorted before being allowed access into the unit (see Section 4.5 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.
- ☐ Internal doors/frames to any offices or back-of-house plant/service/stores etc. within the units 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

- ☐ 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 be fixed with a secure glazing retention system (e.g. with security glazing tape, with a dedicated security sealant/gasket or a secure mechanical fixing system from the glazing retention tests within the BS PAS 24 or LPS 1175 standards)
- ☐ Any 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 SR1/2 and installed in accordance with manufacturer's instructions. Ideally, any external 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

- ☐ The inner pane within double-glazed glazing units at ground floor level should have no less than a 1.5mm PVB interlayer (e.g. 7.5mm laminated glass), or a glass rated as P4A under BS EN 356. The remaining pane in a double glazed unit may be toughened glass.
- ☐ If there are to be any vision panels within loading bay doors that cannot include laminated glazing, they should include a material of a similar strength (e.g. multi-layer acrylic/polycarbonate or hammerglass) to ensure they are resistant to shattering and penetration.
- ☐ There should be a block work wall (or a material of similar strength, such as welded-steel or expamet mesh) behind any cladding to the units, to a minimum height of 2000mm from external ground level, to ensure that the fabric of the building itself is not vulnerable to attack. Internal walls between the units themselves should be similarly robust to prevent unauthorised access from one unit into another.

4.4 Access Controls

- ☐ Access control systems should be operable by swipe card or fob, and not numeric keypads (which can be easily observed/shared and are rarely changed). The following doors/gates should operate on access control:
 - The vehicular gates (and any pedestrian gate) at the access and egress points to the site should be self-closing/locking, controlled on access and egress (i.e. no induction loop) via staff key-fob/proximity reader or via an audio/visual access-control system linked to each unit. The gates should ideally be secured and operate via the access-control system on a 24/7 basis, but at least outside of normal working hours if staff access is required (e.g. 6pm-7am).
 - The main entrance doors to each unit if/when there is no staffed reception (operated by staff card/key-fob and via video access controls linked to a reception/office/warehouse).
 - Any internal doors providing access to obvious high risk areas e.g. server rooms, storage areas, staff changing facilities/lockers etc. (operated by authorised staff card/key-fob only).
- ☐ The electric locking system to be used throughout the site/units 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 Alarms

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

4.6 Boundaries

- ☐ The perimeter of the site should be defined by brick/concrete retaining walls and high security, rigid-panel, welded-wire mesh fencing and gates to a minimum height of 2400mm from external ground level. Any combination of retaining walls and welded-wire mesh fencing should have fencing panels that are fixed flush with the outer skin of the retaining wall below, leaving no steps/gaps that would provide a climbing aid. The fencing panels should be fixed to posts with anti-tamper fixings preventing damage or removal and should ideally be 358 gauge, with small apertures to deter scaling and cutting - see <https://www.securedbydesign.com/member-companies/accredited-product-search> for a list of Police approved perimeter security suppliers. Sliding vehicular gates are preferred to site access/egress points (which are easier to operate and secure remotely), but if double gates must be used they should overlap when closed and should not be capable of being forced open (see Section 4.4 for information on how they should operate).
- ☐ Care should be taken to ensure that any level changes do not inadvertently facilitate climbing or leave large gaps underneath the panels/gates. There should be no centrally located horizontal bars to aid climbing and the gates should be located away from other climbing aids, such as low walls, streetlights, trees etc. Exposed hinges and large sliding bolt apertures/locking points should be avoided, or fitted with shrouding/protective plates (see opposite) to avoid the creation of footholds. The gap at the bottom of any gates should be small enough to stop anyone crawling through.
- ☐ The narrow route to the sides/rears of the units should be secured with 2100mm high secondary fencelines and gates to prevent unauthorised access to the hidden elevations/doors of the units during operational hours. If panic mechanisms are required on the inner face of any pedestrian gates for escape purposes, they should not be capable of being reached/operated from the external face of the fencelines/gates.



- ☐ Care should also be taken to ensure there are no trees or any other hard/soft landscaping features immediately adjacent and on the external 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 the 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.
- ☐ Any low boundaries that adjoin high boundaries should have transition panels/sections to prevent the low boundary being used as a climbing aid over the higher.

4.7 Parking Areas

- ☐ 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 parking areas should be even tarmac or concrete. 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.

4.8 Lighting

- ☐ External lighting must be provided to the access route and parking/servicing areas within the site, in accordance with BS 5489.
- ☐ Fittings should produce 'white' light, as opposed to yellow/orange light. LED 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 and loading bay 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 access/egress points to the site, the main entrances and facades of each unit 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 cycle parking area should be located where it can be well-overlooked from routinely occupied rooms within the units 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 secure, lockable and fire resistant enclosures. 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 or locker areas.

5 Management & Maintenance

- 5.1.1 A comprehensive security regime for the management of the units must be prepared and remain in place for the day-to-day running of the building. 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. The operating/maintenance plan should focus on issues such as:
- Opening and closing the site/units, including staff arrival and departure;
 - Management of deliveries (servicing activities should not require any service doors to remain open unattended for prolonged periods);
 - Details of staff security training;
 - Location and management of any smoking areas;
 - Repairing damaged external and internal fittings, particularly security features e.g. access control systems, alarm systems, CCTV cameras, lighting etc;
 - Cleaning and prompt removal of graffiti, litter etc; and
 - Refuse collection arrangements.
- 5.1.2 Any high value equipment within communal areas (e.g. computers, televisions, tools etc.) should be properly marked and securely fixed or stored to deter damage/theft. An accurate record should be maintained which logs all such items.
- 5.1.3 Refuse collection arrangements should not require bins to be left in the street for extended periods/overnight. Servicing activities should not require any service doors to remain open unattended for prolonged periods.
- 5.1.4 Adequate signage should be deployed in all areas not only to direct people throughout the site/units, but also to deter unauthorised access to staff-only/back-of-house 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
14 th March 2024	Atelier Two	Receipt of CIS instruction form & plans
18 th March 2024	Atelier Two	Quote email sent. Confirmation of instruction & acceptance
15 th April 2024	Atelier Two	Email sent re: report completion & payment
19 th June 2024	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
2434 PL100	Topographical Survey	23.12.23	A
2434 PL101	Site Layout	05.01.23	B
2434 PL102	Proposed Elevations	05.01.23	B
2434 PL103	Ground Floor Plan	05.01.23	B
2434 PL104	First Floor Plan	05.01.23	B
2434 PL105	Proposed Site Sections	05.01.23	B
2434 RP100	Design & Access Statement	Dec 2023	B

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

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.

BS EN 1627 (Security Ratings RC1 to RC6)

Windows, doors, shutters - Burglar resistance Requirements and classification

The classification system used in BS EN 1627 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

Enhanced security requirements for doorsets and door assemblies for dwellings to satisfy the requirements of PAS 24

STS 202

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 LPS 1175.

BS EN 356 (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