HOARE LEA

Manor Farm.
Slough.
Design and Access Statement.

SECURITY

REVISION 02 – 13 DECEMBER 2024

Audit sheet.

Rev.	Date	Description of change / purpose of issue	Prepared	Reviewed	Authorised
01	19/11/24	Initial planning issue	LA	PB	LA
02	13/12/24	Revision 1	LA	PB	LA

Project number: 25-25674
Document reference: 2525674-HLE-XX-XXX-RP-SC-754-003 -Manor Farm Security Site Design and Access Statement Rev02.V1.docx

Contents.

1. Introduction.

This design and access statement has been prepared by Hoare Lea Security team. This report is based on a thorough understanding of both the threats and resultant risks (together with their mitigations), which have been reviewed and agreed by the Designing Out Crime Officer (DOCO) for the Borough of Slough.

During the development of a Security Risk Assessment, a number of operational requirements have been developed. These form the foundation of the security strategy design for the Project.

Guidance and Objectives.

This report was developed to demonstrate that the development has a security strategy which seeks to comply with:

- The National Planning Practice Guidance and the Nation Planning Policy Framework requirements.
- The Metropolitan Police and the DOCO for the Borough of Slough recommendations.
- Secured by Design planning conditions 25 A and B.
- Secured by Design guides (Commercial 2023 and Homes 2024).
- National Protective Security Authority (NPSA) principles.

The NPFF 2023 explicitly addresses the requirement for developments to promote healthy and safe communities which:

1. Promote social interaction.
2. Are safe and accessible so that crime and disorder and the fear of crime do not undermine the quality of life or community cohesion.
3. Enable and support healthy lifestyles.

In providing a space which supports quality of life, this can be further promoted by:

- Anticipating and addressing possible malicious threats and natural hazards, especially where large numbers of people are expected to gather (such as transport hubs, nighttime economy venues, hotels, and restaurants), through the assessment of potential threats and adoption of proportionate steps to reduce vulnerability, increase resilience and ensure public safety and security; and
- Ensuring operational sites are not affected adversely by the impact of other developments proposed within the area.

The National Planning Practice Guidance and the National Planning Policy Framework expresses the importance of addressing crime and its impact on communities, referencing the role of a DOCO in the planning process of a development. The DOCO works with the development's architects, designers, security experts, and the local authority to ensure that the physical security of a building/site is improved by incorporating crime prevention techniques in the layout, landscaping and products used.

1.1 Secured by Design principles and guides.

Secured by Design (SBD) is the official police security initiative working to "improve the security of buildings and their immediate surroundings to provide safe places to live, work, shop and visit." It focuses on the construction of well-designed places, buildings, and communities that promote both sustainable communities and health and well-being, but are also safe, secure, and accessible.

SBD is not anticipated to be a planning condition for the site; however, the site has been designed with the principles and best practices in mind. As a new Data Centre site, key principles from the NPSA shall also form an element of the design considerations to be taken as the project progresses.

1.2 Security Objectives.

The security objectives for Site are as follows:

- Protection of Life.
- Protection of Assets.
- Prevention of all crime events and to minimise their impact if realised.
- Reduction of business interruptions.
- Preservation of essential building services.
- Continuity of primary business operations.

2. Security design approach

The overarching aim of the security design of the facility is to provide appropriate and proportionate security risk mitigation measures that allow users to feel safe and secure. In this way, security can act as a key component in the sustainability and wellbeing aspirations of the development. It should be noted that safety and security is an integral part of the design process and has been considered from the outset.

A formal security risk assessment (SRA) has been undertaken (and will be continually reviewed) that has identified the security risks posed to the development. The adoption of an operational requirements approach allows the treatment strategies to be built around identified security needs and therefore allows for the final security designs to evolve alongside the wider building and landscaping designs, whilst maintaining the strategic intent and justification for the measures. Thus, the requirements identified within the SRA have been appropriately integrated into the security strategy design.

A detailed threat assessment formed part of the SRA which identified the design basis threats from which the security risks are assessed. Throughout the process and subsequent design development there will be ongoing engagement with both internal and external development stakeholders including the following:

- Metropolitan police Design out Crime Officer (DOCO)
- Counter Terrorism Security Advisor (CTSA)
- Design and project teams.

It should be further noted that the landscaping design and vehicle approach is being developed cognisant of the future potential Duty to Protect legislation and developing Protect By Design approach, although based on our understanding of government issued guidance at the time of writing this report, it is unlikely that the site will fall under the scope of this future legislation.

3. Security Design principles.

3.1 Overview.

Protection has been applied to the Project Concorde development and its assets to mitigate security risks, through development of various security risk treatment strategies which are based on the following principles:

- Deterrence: measures to deter those who may be looking to commit crimes or cause a security incident.
- Detection: measures that provide time and space for the detection of breaches in security unauthorised access.
- Delay: measures that impose a delay on those committing crimes or security breaches, increasing the risk of detection and being caught by those responding to the incident.
- Response: controls which provide an effective response to incidents or alarms raised.
- Recovery: measures which support incident recovery.

The evolving security risk treatment strategies are being strongly influenced and informed by recognised best practice design guidance (discussed in Chapter 1) for the creation of sustainable and secure developments and communities. These can be summarised through a number of high-level attributes that the developments should possess in order to successfully create a safe and secure environment. outline a series of high-level attributes that the developments possess in order to successfully create safe and secure environments. These include:

- Access control and movement
- Structure/Infrastructure
- Surveillance
- Ownership
- Physical protection
- Activity
- Management and maintenance
- Lighting.

3.2 SBD and CPTED.

Discussion with the Borough of Slough DOCO has led to an agreement on SBD principles being implemented across the site and within the design.

SBD follows CPTED (Crime Prevention Through Environmental Design) principles with the addition of specific guidance and British Standards relating to physical and technical security measures. CPTED aims to reduce the number of opportunities for crime by effectively designing the built environment. It draws heavily on the behavioural psychology by examining the relationship between people and their environment i.e., a potential offender will assess the environment to make a rational choice, based on the level of risk versus reward.

3.3 Access Control and Movement.

Strategies of access control aim to only allow access to authorised users and deny access to a non-public space, be that due to user experience and safety or a critical asset. This should be implemented in a way that compliments convenient movement of legitimate users without compromising the security. Access control at the West site involves both formal and mechanical strategies.

- Formal access control is more purposeful and organised such as entry procedures and checks carried out by third parties who in their normal functions can deny access. e.g., security personnel and receptionists.
- Mechanical access control involves the use of gates, barriers, and access control systems on doors.

Key attributes within the design of the site includes:

- The site is located to the Western area of nearby Heathrow airport on the edge of an industrial estate development, therefore access links to the M25 motorway is easily accessible, however crime statistic numbers are prevalent with the business types located within the industrial park.
- Pedestrian, cyclists, and vehicle access to the site will be controlled via the site primary entrance and exit point, which will remain under 24/7 security guard occupation.
- The site will have a secure fence-line enclosing the entire site and building assets within.
- Additional security technology system will be deployed to aid in the deterrence, detection, delay, and response to potential incidents.

A layered security approach to the site has been taken to ensure that user experience is maintained whilst maintaining the necessary access restrictions of a well-defined secure space.

3.4 Surveillance.

The security strategy for the site utilises surveillance measures to increase the level of perceived risk by adversaries: a subjective judgement on how likely one may be to get caught carrying out an offence. Surveillance aims to increase the potential for detection, apprehension, and prosecution, as well as deterring adversaries from targeting the site initially. Two forms of surveillance are utilised:

- Formal surveillance is purposeful measures carried out by either video surveillance systems (VSS) or third parties such as security personnel and receptionists. The main purpose is for real-time monitoring of both internal and external areas to support with rapid detection and response to incidences, and to provide a body of evidence i.e., prosecution evidence.
- Informal surveillance focuses on the design of a space to enhance natural surveillance levels and therefore maximise the perceived risk by an adversary. This in turn provides deterrence and reduces the likelihood of a threat occurring.

Lighting can also have a significant impact on the perceived risk in an area as it supports the level of natural surveillance.

Key attributes within the design of the site includes:

- A lighting strategy which integrates appropriate and uniform lighting across the external spaces. This intends to design out dark spaces and create a feeling of safety for legitimate users, as well as enhancing the capability of natural surveillance.
- The site location may prove difficult to illuminate due to ecological factors, therefore different surveillance and detection technology measures may be required to be deployed (Infra-Red lighting/ Thermal cameras etc)
- Where natural surveillance is limited and/or a space would benefit from additional surveillance, video surveillance (CCTV/VSS) will be used to support the security of the site.
- Video surveillance systems will be strategically placed and co-ordinated with both the lighting and landscape designs to limit blind spots.

3.5 Physical protection.

Effective physical security measures across the Site intends to increase the robustness of the site perimeter as to protect the people and valuable property within, through implementation of measures which are both commensurate to the level of risk and well-designed.

Key attributes within the design of the site includes:

- Robust yet proportionate physical measures with a focus on integration with the development design from the offset, rather than a 'bolt-on' approach
- Protection of the most valuable assets across the site (as per the security risk assessment) and in accordance with SBD guidelines agreed with the DOCO and in accordance with NPSA guidelines for CNI sites.
- Robust physical security boundary and clear demarcation of owned land areas.
- Physical landscaping designs will be adapted where appropriate to increase the security posture to deter and maintain levels of natural surveillance where possible.

The design of the physical protection strategy will be aligned to the principles of protection in depth and be proportionate to the identified security risks.

4. Summary.

The site development proposes to create a safe and secure environment through the application of industry best practice security design principles such as Crime Prevention Through Environmental Design (CPTED) and the Police Service's Secured-By-Design initiative (noting that a Secured-By-Design Application will not be submitted for this development). In doing so, it adheres to the requirements of the NPPF and NPSA guidelines for Critical National Infrastructure (CNI) and Data Centres. The requirements of security have been balanced against the desired function and use of the space, as well as the context of the surrounding area.

This approach to security will positively influence the project to deliver a robust and secure site, whilst ensuring there is no detrimental impact to the surrounding developments.

HOARE LEA

LIAM ARMSTRONG
SENIOR ASSOCIATE

+44 1865 670382
liamarmstrong@hoarelea.com

HOARELEA.COM

Royal Exchange
Manchester
M2 7FL
England