Physical Security Standards Policy (Surrey and Sussex) (1208/2025)

Abstract

This policy details the Forces physical security controls for individuals, information, materials, and infrastructure.

Policy

1. Introduction

The objective of this policy is to prevent any unauthorised physical access, damage and interference to Surrey Police and Sussex Police (hereafter referred to the Forces) premises, information, and assets.

2. Scope

2.1 Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent any unauthorised access and the protection of the Forces, our people, information, materials, and infrastructure.

2.2 This policy and procedure apply to all who are authorised to access Forces' information and operational assets including but not limited to the Forces' staff, police officers, volunteers, staff working in the Office of the Police and Crime Commissioner, delivery partners and third party contractors.

3. Policy Statement

3.1 The Forces will put into place, or build into the design, measures that prevent, deter, detect, and delay attempted or actual unauthorised access, acts of damage and/or violence; and that trigger an appropriate response.

3.2 Each site will be risk assessed to determine the level of controls which will depend on different factors such as the nature of the threat, the cost effectiveness of the controls, the site, and its surrounding environment, whether it is sole or shared occupancy or has public access. The physical security controls may, therefore, be different for each location and it is important that the correct type and mix are implemented.

3.3 The Forces have adopted Secured by Design (SBD) as the official standard for physical security. Physical security recommendations will therefore always consider SBD rated products first, subject to review from stakeholders.

Procedure

1. Introduction

1.1 This procedure is a key component of the Forces' overall security management framework and should be considered alongside more detailed security documentation including clear desk, clear screen, security incident handling, visitors, and the remote and home working procedures. Refer to Surrey Police and Sussex Police Information Security Policy (722).

1.2 The purpose of this document is to set out the requirements for consideration when establishing and maintaining secure working environments. The physical security requirements of any location are derived by the sensitivity of the information or operational assets protected within. This procedure is intended as a general guide to physical security; it does not provide a specific guide for all eventualities. If further information is required, please contact the Security and Information Assurance Team.

1.3 The objective of this procedure is to prevent any unauthorised physical access, damage and interference to the Forces' premises, information, and assets.

1.4 The aim of this procedure is to:

• address threats from criminals, organised criminal groups, terrorists, disaffected individuals, employees or groups and other threat sources;

• ensure critical or sensitive information processing facilities and operational assets are housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls; and

• ensure compliance with the Forces' insurance policy conditions of cover. (For detailed insurance guidance on the conditions contact the Force Insurance and Risk Management Team.)

2. Physical Security Working Practices

2.1 Good physical security relies on maintaining a secure working environment and following secure working practices.

2.2 It is important to be aware of the risks associated with any working environment and to ensure that personal data, sensitive police information, and operational assets are protected at all times.

2.3 The physical security arrangements of all police working environments must be assessed by the Security and Information Assurance Team to ensure they are suitable for processing police information. These environments are typically police owned / leased offices or shared / third party offices. The Security and Information Assurance Team will conduct a risk assessment to ensure the security controls applied are proportionate to the potential threats to the assets. This will also enable a record to be kept of tolerated exceptions which the team will review at each point a site is revisited to determine if such exceptions are still appropriate. The physical security requirements must be agreed and implemented before new offices are approved and wherever office moves or significant changes take place.

2.4 Temporary, remote working or home working environments do not require an assessment if using Force supplied mobile working facilities in accordance with these

procedures. Line Managers must ensure that individuals working from home are made aware of how to keep their equipment and working environments secure (See Surrey Police and Sussex Police Information Security Policy (722) Remote and Home Working Procedure.) Guidance can be sought from the Security and Information Assurance Team.

2.5 Everyone is responsible for the ongoing review of the security of their environments and ensuring that colleagues and delivery partners are handling police information and operational assets securely. Any defect in physical security must be reported to the Estates and Facilities team immediately to repair. Serious weaknesses or breaches that could have compromised police information, and/or could affect the wider police estate, should also be reported to the Security and Information Assurance Team in accordance with the Security Incident Management Procedure, an Appendix to the Surrey Police and Sussex Police Information Security Policy (722).

2.6 Office moves and changes can present a serious risk to the protection of the Forces' information. Particular attention must be paid to identifying all personal and sensitive information that is affected by the change and ensuring that it is protected at all times. Unit managers are responsible for ensuring that all containers, rooms, and buildings have been thoroughly checked and that there are clear plans in place for ensuring that the information remains protected during and after any moves or changes, and that any relocation of the information is carried out securely.

2.7 Departments should also consider the security procedures controlling the storage and handling of information relating to the Forces' physical infrastructure; for example, floor plans, construction details, network maps, emergency procedures etc., which if placed in the wrong hands could compromise physical security. This requirement will also apply to contractors and/or third parties who have access to such information.

3. Buildings and Perimeters

3.1 In any building in which information or operational assets are stored there should be as few points of exit and entry as possible (allowing for the functions of the building and safety.) Physical protection can be achieved by creating several physical barriers around premises and offices. Each barrier establishes a security perimeter and increases the total protection provided. The position, strength and number of barriers should be appropriate to the assets to be protected, as determined by a risk assessment conducted by Security and Information Assurance, in collaboration with stakeholders from Estates and Facilities.

3.2 The following controls should be considered and implemented where appropriate:

The security perimeter should be clearly defined. These can include barriers such as fences, walls or hedges, card entry gates / doors, rising arm road barriers, key / pin-controlled entry points or staffed reception areas. Appropriate signage can also help to create a security perimeter through effective demarcation between public and private areas.

3.3 Perimeters of buildings or a site should be physically sound, in a state of good repair (i.e., there should be no gaps in the perimeter or areas where a break-in could easily occur to restricted areas e.g., secure car parks, garages or storage facilities) and notices displayed to indicate that access is restricted to authorised personnel only e.g. No Public

Right of Way, Authorised Personnel only after this point or no unauthorised access. Signs must not identify the presence of sensitive information or assets.

• All external walls should be of solid construction.

• Windows and external doors should be in a state of good repair, structurally resistant to forced access and protected by control mechanisms, such as bars, alarms, or locks. Doors should be fitted with automatic door closers and doors and windows must be locked when areas are unattended. Lock and key management processes must be put in place for out of hours, or when offices or rooms are not in use.

• Where used as a security barrier, door hinges must be on the inside.

• External security on doors should be via a catch style electronic pass system that auto closes with minimal delay. Where it has not been possible to install an electronic access pass system to an external door and a code system is used instead, codes should be changed every 6 months, or whenever an individual no longer needs access to the premises, as a minimum.

• Physical barriers should, where relevant, extend from real floor to real ceiling in order to prevent unauthorised entry or environmental contamination such as that caused by fire and flooding.

• All final entry / exit fire doors should be monitored and tested to establish the required level of resistance in accordance with BS Standards. They should also operate in accordance with fire regulations in a failsafe manner.

• Where there is a requirement for a building alarm determined by Security and Information Assurance and Estates and Facilities, all external doors need to be connected to the alarm system to ensure activation in the event of an intruder.

• Access between the public and the information processing areas of the Forces' premises should be minimised and controlled.

• Additional protection should be considered for windows, particularly those with easy external access such as ground floor windows and those adjacent to flat roofs, or that may be susceptible to drone intrusion. Where premises are closely overlooked by neighbouring buildings or in close proximity to areas where the public have access e.g., footpaths or roads, consideration should be given to ensuring windows have blinds or they are coated in frosted or mirrored film to prevent police information being seen e.g., computer screens or notice boards. An alternative option is the use of computer screen security filters.

3.4 Consideration should be given to the deployment of Close Circuit Television (CCTV), in particular whether such equipment is to be used to:

• Detect an intruder within a reasonable time frame; or

• Monitor intruders via Force Control Room or external monitoring station; or

• Provide evidence suitable for use in a subsequent investigation or court proceedings.

Advice may be sought from your local Designing Out Crime Officer, a Counter Terrorist Security Advisor or from the Security and Information Assurance Team. Any requirement for CCTV must also be supported by lighting that is effective and fit for purpose. (Also see section 6.4 for CCTV considerations where sensitive assets are involved).

All CCTV must be implemented to meet the requirements of the Forces' CCTV Specification.

Outdoor lighting conditions should be reviewed in conjunction with CCTV deployment to enable enhanced monitoring condition in hours of low light / darkness.

3.5 Hazardous or combustible materials should be stored securely at a safe distance from any secure area.

3.6 Fall back equipment and/or back up media should be sited in a suitable location in order to prevent it from sustaining damage from any disaster occurring in the main site.

4. Physical Entry Controls

4.1 The following controls are required:

• Any visitor, including third party contractors, must be pre-notified to Front Counter or Reception and (where there is one), on arrival, register and be issued with a visitor's pass.

• It is the responsibility of the Forces' employee who is being visited to ensure that their visitor is supervised at all times during their visit.

• On departure, the Forces' employee must ensure the visitor's pass is withdrawn and the time and date of departure is recorded.

• Access to sensitive information and offices must be controlled and restricted to authorised personnel only.

• All Forces' personnel, contractors and visitors are required to wear their identity passes when on police premises.

• It is the responsibility of all staff to challenge any individual that they encounter on Force premises who is not wearing visible identification. Any individual who, on being challenged, is unable to produce a Force identity card or visitor's pass should either be escorted to the reception area or remain accompanied while enquiries are made into the legitimacy of their presence. Note the Force's Guidance on the presence of Auditors / Social Media Bloggers.

• When an officer or member of staff (including volunteers) leaves Force employment it is the responsibility of the line manager to ensure the identity card and any Force assets in their possession are returned, in addition their access to Force premises and any access

to Force computers needs to be revoked. Leavers Process (Sussex), Leavers Process (Surrey).

Access rights to secure areas should be regularly reviewed and updated but especially when staff members move or leave.

5. Car Parks

5.1 External Lighting should be available to ensure the security and safety of personnel and vehicles during hours of darkness. Location and coverage of lighting should be decided in collaboration between Estates and Facilities and Security and Information Assurance.

5.2 Wherever possible, and for any newly built car parking facilities, alignment with the Park Mark Accreditation scheme should be sought.

5.3 Staff using Forces' car parks should only do so if they are authorised to use them and working. Cars should not be left on site for prolonged periods or overnight if the member of staff is not working at the time.

5.4 Only vehicles authorised to park on site will be allowed access through secure entry gates / barriers (where appropriate). Fleet vehicle users must display the vehicle logbook on the dashboard. Other vehicle users are required to ensure their contact details are accessible or on display in the vehicle.

6. Storage of Sensitive Assets

6.1 Critical, high-value or sensitive assets must be housed in secure areas, protected by a defined security perimeter, with appropriate security and entry controls. The protection provided should be proportionate to the identified risks and the security classification given to the assets.

6.2 A secure area may be a locked office or several rooms within a physical security perimeter. This may be locked and may contain lockable drawers, cabinets, or safes. The selection and design of a secure area should take into account the possibility of damage, unauthorised access, fire, flood, explosion, and other forms of natural or human-made emergency. Account must also be made to the relevant Health and Safety regulations and standards.

6.3 Additional controls and guidelines are required to enhance the security of a secure area processing assets classified as OFFICIAL SENSITIVE or above. These include controls for the personnel and any third parties working in the secure area.

6.4 The following controls may be considered:

• Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis.

• Unsupervised working within a secure area should be minimised, both for safety reasons, and to prevent opportunities for malicious activities.

• Vacant secure areas should be physically locked and where possible alarmed.

• Third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when necessary. They will either need to be appropriately vetted or escorted at all times.

• Consideration should be given to additional barriers and perimeters between areas of different security requirements inside the security perimeter e.g., intruder detection alarms, enhanced locks or entry controls, CCTV monitoring, enhanced secure storage containers or safes. The Security and Information Assurance Team can provide specific guidance as part of their risk assessment.

• Photographic, video, audio or other recording should not be allowed unless authorised. Where authorisation has been obtained, use of such equipment should be strictly controlled.

• For CCTV, the coverage needs to be considered against the security of the environment without compromising the security of systems and access (such as viewing a terminal screen that views sensitive system data) and should align to the Surveillance Camera Commissioner Code of Practice.

• Shared support functions and equipment (e.g., photocopiers / printers, stationery stores) should be sited outside the secure area in order to avoid demands for access that may compromise sensitive assets. Secure areas should have their own equipment.

7. Equipment Security

7.1 The protection of equipment, including mobile equipment and that used off site, is necessary in order to reduce the risk of unauthorised access to data and to guard against loss or damage.

7.2 Equipment should be sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access.

7.3 The following controls are recommended:

• Output equipment, such as monitors and printers, should be positioned to reduce the risk of sensitive information being viewed or obtained by unauthorised personnel.

• Measures should be in place to minimise the risk of potential threats, for example from theft, fire, explosives, water (or water supply failure), dust or chemicals.

• There should be no consumption of food or drink in the vicinity of major processing equipment (i.e., servers, hubs, and routers). Sensible precautions should be taken to avoid the spillage of food or drink on other equipment.

• Environmental conditions should be monitored for elements that might adversely affect the operation of information processing facilities.

• The potential impact of a disaster happening in nearby premises should be considered.

8. Power Supplies

8.1 Critical equipment for priority services should be protected from power failures and other electrical anomalies. The electrical supply to all Forces' equipment should conform to the equipment manufacturers' specifications.

8.2 The Forces' networks are provided with an Uninterruptible Power Supply (UPS). Where practicable, other Force equipment providing critical Force operations should also be supported by a UPS in order to support orderly close down or continuous running. UPS equipment should be regularly checked to ensure that it has adequate capacity and tested in accordance with the manufacturer's recommendations.

8.3 Lightning protection should be applied to all buildings that house assets / information or activity susceptible to lightning strikes. Lightning protection filters should be fitted to all external communications lines.

9. Cabling Security

9.1 Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

9.2 The following controls are recommended:

• Power and telecommunications lines into information processing facilities should be underground, where possible, or provided with alternative protection. Access to underground cabling, for example via manhole covers, should be secure and tamper-poof.

• Network cabling should be protected from unauthorised interception or damage by measures such as conduit or by avoiding routes through public areas.

• Power cables should be segregated from communications cables to prevent interference.

9.3 For sensitive or critical systems, further controls may include:

• Armoured conduit and locked rooms or boxes at inspection and termination points.

• Use of alternative routings or transmission media.

• Use of fibre optic cabling.

• Sweeps for unauthorised devices being attached to cables.

10. Equipment Maintenance

10.1 Forces' equipment should be correctly maintained to ensure its continued availability and integrity.

10.2 The following controls are required:

• Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.

• Maintenance should only be carried out by Forces' staff or by authorised third party contractors.

• A record of all suspected or actual faults or power supply failures affecting the Forces' network and the telecommunications system is maintained by the IT Service Desk.

• Wherever practicable, Forces' equipment, particularly that containing stored data should be repaired or maintained on Forces' premises. Appropriate controls should be implemented where it is necessary to send equipment off premises for maintenance.

11. Security of Equipment Off-Premises

11.1 The security of Forces' IT equipment away from Forces' premises should be equivalent to on-site equipment used for the same purposes but should take into account the additional risks of working away from Forces' premises (see the Remote and Home Working Procedure an Appendix to the Surrey Police and Sussex Police Information Security Policy (722)).

12. Secure Disposal or Re-use of IT Equipment

12.1 All disposal or re-use of IT equipment must be in accordance with the Disposal of Storage Media Procedure an Appendix to the Surrey Police and Sussex Police Information Security Policy (722).

13. Selection of Security Controls and Equipment

13.1 The Security and Information Assurance Team can provide advice and guidance with regard to the selection of security controls or security equipment, e.g., doors, locks, CCTV etc. The Team can do this informally via general enquiry, or formally through a documented site review and risk assessment. The assessors will base any recommendations upon standards and guidance issued by Secure By Design or the National Protective Security Authority (NPSA). As stated, the selection of the security controls will depend upon the threat and risk. In some cases, for example to protect our most sensitive or high value assets, the use of Product Assessment Specification (PAS) or Loss Prevention Standard (LPS) rated products will be appropriate and advice can be sought from the local Designing Out Crime Officer or Counter Terrorist Security Advisor.

14. Physical Security Governance

14.1 The Security and Information Assurance Team are responsible for setting the standards for the management of physical security and own this policy and procedure. The Estates and Facilities Team are responsible for implementing the standards across the Force estate. For shared premises, the required security controls and standards must be set within the terms of the agreement.

14.2 Matters relating to the physical security of the estate are discussed and escalated where necessary at the Security and Information Management Board (SIMB) chaired by the Chief Operating Officer.

Team: Security and Information Assurance.