Security Standard – Physical and Electronic Security (Part 1)

Enterprise Security Risk Management -

Physical Security Team

Department for Work & Pensions

Date: November 2022

Contents

1. Revision History

Version	Author	Description	Date
0.0a / 0.0f	ESRM PST	First Drafts	25/11/2021
0.0e	ESRM PST	Incorporating comments from Stakeholders	04/01/2022
0.0f / 0.0j	ESRM PST	Further iterations	25/01/2021
0.0k	ESRM PST	Incorporating External Best Practice Feedback	18/03/2022
0.0l	ESRM PST	Final amendments from Estates and Health & Safety Stakeholders	14/04/2022
0.0m / 0.0n	ESRM PST	Amendments results from SPAG Review	25/04/2022
1.0	ESRM PST	First published version	05/05/2022
1.1	ESRM PST	Amended to amend some CPNI requirements to align with HMG MPSS	24/10/2022

2. Distribution

Version	Role/Area	Role	Date

3. Approval History

Version	Approver Title	Role	Date
1.0		DWP Security Policy Assurance Group	05/05/2022
1.1		DWP Security Policy Assurance Group	16/11/2022

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status and at least annually thereafter or whenever there is a significant change that requires impacting.

4. Introduction

4.1. This Standard provides the list of outcomes required to define security implementations to a defined level. This Standard provides a list of security controls to minimise risk from physical threats to assets.

4.2. Furthermore, the security controls presented in this Standard are taken from Governmental best practice for physical security, including ensuring close alignment with Government Functional Standards GovS 007 (Security) and GovS 004 (Property) and have been proportionately tailored for DWP, DWP Contractors, and all DWP Suppliers.

4.3. This document does not recommend any particular security manufacturer – the focus is on capability and suitability to requirements.

5. Purpose

5.1. The purpose of this document is to define security requirements that can be deployed and managed to a set of standards. This includes providing guidance as appropriate to suppliers.

5.2. Security Requirements **MUST** have a Security Risk Assessment / Site Security Plan in place for the defined physical controls.

Best practice is to utilise the CPNI **Operational Requirement (OR)** process. The process helps organisations make smarter investment decisions in protective security measures, enabling them to implement measures which are in proportion to the risks they face.

The resultant Operational Requirements follow the layered security principles:

- Deter - stop or displace the attack.
- Detect - verify the attack and initiate a response.
- Delay - prevent the attack from reaching the asset (including measures to minimise the consequences of an attack).
- Mitigate – minimise the consequences of an attack against your site.
- Respond – actions to prevent the goal of the attack being completed.

The output from the OR process will help define the necessary security measures required for a site. The output from an OR process will be a Security Risk Assessment and Site Security Plan.

6. Exceptions

6.1. Any exceptions to the application of this Standard **MUST** be risk assessed and **MUST** be presented to the organisation risk owner to allow a risk treatment decision.

6.2. Exceptions to this Standard **MUST** be maintained on a risk register for accountability, traceability, and reporting.

7. Audience

7.1. This Standard applies to all DWP sites, suppliers and contracted third parties.

8. Scope

8.1. This Standard applies to Physical Protection Systems handling DWP Assets as defined in Section 10.

9. Assurance

9.1. Controls referred to or presented in this Standard, will be subject to formalised reviews and security audits to provide evidence of adequacy and effectiveness.

9.2 This document **MUST** be annually reviewed by Competent and Experienced Personnel as a minimum.

10. Definitions

"MUST"	Means that there is an obligation to perform the activity.
"MUST CONSIDER"	Means that there is an expectation that the activity will be performed. There can be rare exceptions when the activity is not performed. There MUST be a clear process in place to document and manage risks.
"MUST NOT"	No activity should take place.
"Asset"	An asset is any property, people and information with a classification which is the responsibility of DWP and its suppliers.
"Security Key"	A key used to access external building doors, utilities, secure rooms, information with a classification, and other areas of higher sensitivity.
"Zoning"	Breaking down areas of a site or facility to better define the Physical Controls required based on the function of each area.

11. Glossary

AACS	**Automated Access Control System**
ARC	**Alarm Receiving Centre**
BASE	**CPNI rating against a forcible attack**
BOH	**Back of House**
BCP	**Business Continuity Plan**
CIS	**Computer Information Systems**
CLASS	**CPNI rating against a surreptitious attack**
CSE	**The Catalogue of Security Equipment**
CT	**Counter Terrorism**
CTM	**Counter Terrorism Measures**
DFA	**Dual-Factor Authentication (a token presented by user with additional pin code, or biometric reader for example)**
DWP	**Department for Work and Pensions**
HMG SPF	**Her Majesty's Government Security Policy Framework**
HVM	**Hostile Vehicle Mitigations**
ICT	**Information Communication Technology**
IED	**Improvised Explosive Device**
IDS	**Intruder Detection Systems**
MEP	**Main Entry Points**
MOP	**Members of the Public**
OOH	**Out of Hours**
OR	**Operational Requirements**
PIDS	**Perimeter Intruder Detections System**
PST	**Physical Security Team**
QEP	**Qualified and Experienced Persons**
REEP	**Rapid Estate Expansion Programme**
RM	**Risk Management**
RMF	**Remote Monitoring Facility**
RMP	**Risk Management Process**
SAMS	**Security Access Management Systems**
SCR	**Security Control Room**
SEP	**Staff Entry Points**
SPF	**HMG Security Policy Framework**
SRM	**Security Risk Management**

SSP	**System Security Policy**
SyOPs	**Security Operating Procedures**
TA	**Threat Assessment**
URN	**Unique Reference Number**
VBIED	**Vehicle Born IED (Improvised Explosive Devices)**
VAW	**Vehicle (used as) As Weapon**
VSB	**Vehicle Security Barrier**
VACP	**Vehicle Access Control Point**

12. Site Security Zoning Methodology and Physical Security Application

When considering physical security, the different areas of a site must be identified as part of any Security Risk Assessment or Site Security Plan. These areas may need different security measures installed**.**

Reference	
12.1	a. Site zoning **MUST** be integrated when applying physical security measures. b. To achieve effective physical security of assets, physical protection measures **MUST** adopt the layered-approach to security (defence-in-depth principles). c. Site Zoning Areas **MUST** at a minimum be assessed for: • Outside the Perimeter (e.g., approaches). • Perimeter. • Inside the perimeter (e.g., landscaping, car parks). • Building (e.g., exterior and interior).
12.2	The following physical security features in each area **MUST** be reviewed: ● Building fabrics (where appropriate) ● Windows ● Entry points and portals ● Internal doors ● Locks ● Barriers ● Access control ● Lighting ● Electronic Security

13. Perimeter

The perimeter is defined as the physical line demarcating the extent of a site/building using a physical barrier and access points providing a means of entering/exiting for people or vehicles.

Reference	
13.1	Perimeter Protective Measures **MUST** deter threat actors from conducting an attack by making each element within the boundary line appear too physically/technically difficult to overcome without likelihood of detection/failure/capture.
13.2	All perimeter access points **MUST** be controlled by physical or electronic measures (such as Automated Access and Control Systems (AACS)) to reduce the risk to assets.
13.3	The number of access points through the perimeter (e.g., gates), especially for locations where there is not a permanent guard force presence or oversight, **MUST** be minimised.
13.4	Access points **MUST** be secured out of hours to maintain perimeter security.
13.5	Gates **MUST** be compliant with the Equality Act 2010 (DDA)
13.6	Where fences are installed, they **MUST** conform with British Standard (BS) **BS1722** Fences (Part 10, 12, 14, 17) specifications: a. Fences **MUST** be a minimum of 1800mm high from top to bottom. b. Fence material will be determined by the Security Risk Assessment or Site Security Plan developed from the OR process. c. Further specifications are available on request.
13.7	Perimeter Lighting **MUST CONSIDER** environmental and technology factors when installed as part of any perimeter installation.
13.8	Lighting **MUST** comply with **BS8418** 4.3.2 CCTV Lighting illumination which defines: • “Camera fields of view **MUST** be illuminated so that it is possible for an operator to verify the presence or absence of a human form in daylight and, if required, in darkness.”
13.9	All entry point doors or portals **MUST** be a barrier that shows evidence of compromise or attempted compromise.

13.10	The door or portal **MUST** deter and delay an attacker and Loss Prevention Standard (LPS) 1175 can be used to assess ratings of resistance.
13.11	On perimeters adjacent to public rights of way, any windows **MUST** be obscured to prevent oversight of information or assets classified as OFFICIAL or higher.
13.12	Organisations **MUST CONSIDER** the following British Standards at a minimum in the installation of perimeter systems. • **LPS 1175** • **BS8418** 4.3.2 CCTV Lighting • **BS1722** Fences

14. Buildings

Building fabric and design can help reduce the effect of threats and protect assets through consultation and the Operational Requirements process.

Reference	
14.1	Organisations **MUST** ensure the building fabric choice for new facilities and refurbishments are led by the Operational Requirements process and consulted upon before construction. Secured by Design principles **MUST** be followed.
14.2	Organisations **MUST** laminate windows (glazing) externally and internally, especially in vulnerable areas, to minimise the damaging effects of secondary fragmentation caused by an explosion, and delay attempted forced entry.
14.3	Laminated glazing **MUST** be included in refurbishment work plans, subject to satisfying legal requirements such as listed building consent.
14.2	Building security measures **MUST** include an intrusion detection system and CCTV coverage that is supported by lighting and signage.
14.3	In some cases, an operational 'front line' (front of house) service will be required at a location where non-front line (back of house) office staff are also based. In these circumstances the services **MUST CONSIDER** self-contained areas with an entrance and reception area that is separate from the main staff and a visitor entrance for that location.
14.4	All non-public facing entry/exit points **MUST** always be locked.

14.5	All access points **MUST** comply with fire regulations and local building controls and allow egress during emergencies
14.6	Doors and Locks **MUST** meet the following standards on main building entry points: a. **BS EN 1303**:2015 Standard - Thumb-turn cylinder lock **MUST** be used at a minimum for main entry points. b. **BS 3621**:2007 Standard – 5 Lever Lock Mechanism **MUST** be used at a minimum where additional door security is required for main entry points. c. **LPS1175**
14.7	Whilst door fabric will be determined by the Operational Requirements process and function, all doors and locking solutions **MUST** equal the same security ratings.

15. Guarding

A guard force is a staffed resource designed to provide immediate Security deterrent and response to threats and incidents. Any guard force must meet the minimum requirements within UK (United Kingdom) legislation.

Reference	
15.1	Any guard force **MUST** be licenced by the **Security Industry Authority** (SIA) to a minimum level of the “Security Guard” licence.
15.2	Any guard force involved in the use of monitoring CCTV **MUST** be SIA licenced to the level of “Public Space Surveillance” licence.
15.3	Where deployed, a guard force presence **MUST** be always on site during standard building operating hours and be flexible to the business need.
15.4	Guard force personnel **MUST** be trained to interact with people, including how to approach and question unusual behaviour and challenge unrecognised or out of date identification/access passes. This training **MUST** be refreshed in line with SIA guidance and contract.
15.5	The guard force **MUST** have sufficient equipment to carry out their duty including communications equipment to be able to respond and alert other guards or authorities to a threat or incident (i.e., radio or mobile device).

Reference	
15.6	Organisations **MUST CONSIDER** the following British Standard as a minimum in the selection of guard forces: • **BS 7499:2020** Static guarding security services • **BS 7984-3:2020** Mobile security services

16. Visitor and People Management

Visitor Management is a key process in controlling access to sites and assets.

Reference	
16.1	Visitors **MUST** be logged with the host. The behaviour of the visitor is the responsibility of the host. The host **MUST CONSIDER** if escorting is required. A method of displaying a visitor pass or token **MUST** be in place.
16.2	There **MUST** be a process in place to log visitors off site and collect any token or pass issued during the visit.
16.3	Staff **MUST** always wear their building pass, visibly, inside their premises.
16.4	Staff **MUST** report any missing or stolen building pass to their Security contact immediately.
16.5	There **MUST** be a process for control of access or building pass tokens.
16.6	Staff **MUST** not wear their building passes or identification outside of the workplace
16.7	When not required display passes **MUST** be stored securely.

17. Server and Communications Rooms

Physical protection measures are required to protect all types of communications, associated servers and network devices from attack, or any access by unauthorised persons.

Reference	
17.1	The following **MUST** be conformed with: a. Server and Communications Rooms **MUST** offer protection against attack and **MUST** resist forcible entry. Design of the doors, locks, floors, ceilings, walls, glazing, and electronic security are to be considered as a single solution. b. Security measures such as IDS, AACS and CCTV **MUST** be used as part of the protective security associated with Server and Communications Rooms. c. Physical security measures **MUST** protect the confidentiality, integrity, and availability of all communications and information systems contained within Server and Communications Rooms. d. The doors to Server and Communications Rooms **MUST** be kept locked when not in use or under close supervision. e. Careful consideration **MUST** be given to the practice of labelling/identifying Server and Communications rooms. It is NOT good security practice to label or identify these rooms, all those requiring legitimate access should be aware of location. f. Security equipment used for daily operations **MUST** not be stored in Server and Communications Rooms as routine, limiting the need for regular unsupervised access to vulnerable equipment. (e.g., Radios). g. Any Server and Communications Rooms with windows accessible from the ground floor or easily accessible upper location **MUST** have additional security measures installed.
17.2	Equipment such as servers and network devices **MUST** be secured in locked security containers or racking, the keys of which **MUST** be treated as security keys and stored accordingly (*Section 18 refers*).
17.2	External air conditioning units **MUST** be protected by security cages.

18. Protection of Protectively Marked Assets

Some assets are afforded protection to a greater degree due to their sensitive nature. Types of physical assets concerned include security keys and protectively marked personal data in all mediums.

Reference	
18.1	Physical assets assessed to be of a more sensitive nature will require more stringent physical controls: a. Assets with a protective marking (PM) above OFFICIAL **MUST** be stored to a greater degree. DWP and suppliers **MUST** adhere to the Government Classification System. b. When not in use, Security Keys **MUST** be stored in a wall mounted container or key box. c. Spare/duplicate keys to security locks **MUST** be held centrally, in approved security containers, by a designated member of staff. d. Keys **MUST** be labelled to facilitate their issue and muster. The labelling **MUST** avoid easily identifying the container to which the key belongs. Key issue **MUST** be recorded.
18.2	Assets **MUST** be managed to meet the following basic principles: a. Compliance with all applicable legal and regulatory obligations: **General Data Protection Regulation (GDPR) and Data Protection Act 2018**. b. Sensitive assets **MUST** be stored in a locked secure container. c. Where protectively marked assets are taken outside the office environment they **MUST** be protected in transit and stored securely. d. Where the impact of loss or compromise has increased because of aggregation, these aggregated data sets **MUST** be secured with DWP approved containers. e. Information that is not freely available in the public domain **MUST** be destroyed in a way that makes reconstitution unlikely. f. Commercial assured facilities that destroy classified information **MUST** be accredited to the following International Organisation for Standardisation (ISO) standards: • **ISO 9001** Quality Management System • **ISO 14001** Environmental Management System • **ISO 18001** Health and Safety Management System

19. Closed Circuit Television and Body Worn Cameras

CCTV systems offer surveillance and enable the “Detect” element, while also acting as a deterrent in accordance with the Deter, Detect, Delay and Respond Security methodology. This can include internal, external and Body Worn Cameras.

Reference	
19.1	To Deter and Detect, CCTV systems **MUST** be designed and installed by a suitably qualified establishment, such as an NSI Gold accredited Security Systems Installer or equivalent.
19.2	CCTV systems **MUST** have a detailed plan defined for each camera location to define the purpose and image target requirements (such as monitor, detect, observe, identify, inspect). This **MUST** allow for the potential usage in prosecutions.
19.3	Audio recording taken from audio enabled CCTV and Body Worn Cameras **MUST** be of sufficient quality for prosecution purposes and be free of background interference. The audio footage **MUST** be able to be associated to the CCTV footage.
19.4	The CCTV system **MUST** be designed and installed to comply with the latest editions of all relevant British and European Standards, codes of practice and statutes: Codes of Practice: a. Information Commissioner Office – CCTV. ICO CCTV. b. Home Office Surveillance Camera Code of Practice. Home Office Surveillance COP. c. UK Police Requirements for Digital CCTV Systems NSI (National Security Inspectorate). d. NACP104 Code of Practice for design, installation and maintenance of CCTV systems, or equivalent accreditation requirements. e. In Scotland: A National Strategy for Public Space CCTV in Scotland. Statutes: f. General Data Protection Regulation (GDPR) g. Data Protection Act 2018. h. Investigatory Powers Act (2016).

Reference	
19.5	For CCTV systems the following **MUST** be reviewed: a. The areas to be monitored such as external perimeter, main entrance, or staff entry point. b. The purpose for monitoring those areas, e.g., if used for access control, the CCTV operator **MUST** be able to positively identify a person or vehicle. c. The picture definition required in each area monitored. d. Where Security System Design defines linkage to an IDS is required. e. The proposed monitoring requirements. f. Maintenance requirement and/or contract arrangements. g. System security measures such as anti-tampering, lightning protection or UPS. h. Access to any CCTV recorder, monitor and associated equipment is controlled. i. Environmental conditions such as lighting, adverse weather etc. and their effect on camera capability. j. Retention periods for CCTV and audio footage **MUST** be defined.
19.6	Organisations **MUST CONSIDER** the following British Standards as a minimum in the installation of CCTV systems: • **BS EN 62676** Video surveillance systems for use in security applications. . • **BS8418** Installation and remote monitoring of detector-activated CCTV systems, Code of Practice. • **BS7958** Closed Circuit Television (CCTV), Management and Operation Code of Practice.

20. Automated Access and Control System

AACS are used to control access points and provide audit trails. AACS can control both access at the site perimeter level and movement within the building.

Reference	

20.1	AACS **MUST** be comprised of the following: a. Security Access Management System (SAMS); the brains of the AACS which connects and communicates with all other key components. b. Kiosk: the interface between the control system and the person administering the system, with role-based access controls to allow for different tiers of administrative access. c. Token: the electronic key, often referred to as a pass or ID which forms one element of the authentication process. d. Reader: is the lock to your electronic key, it communicates with the control system when a key [*valid or not*] is presented.
20.2	AACS systems **MUST** be designed and installed to comply with the latest editions of all relevant British and European Standards, codes of practice and statutes. These, where applicable, include but are not limited to, the following: a. General Data Protection Regulation (GDPR). b. Data Protection Act 2018. c. National Security Inspectorate NACP109 Code of Practice for design, installation and maintenance of access control systems, or equivalent accreditation requirements. d. Equalities Act 2010.
20.3	With any AACS, the following **MUST** be defined: a. Requirements for integration with CCTV within the design. b. Requirements for integration with IDS within the design. c. Interoperability with any other electronic security measures in use currently, or in the future. d. Suitability of physical assets to be installed for example, the robustness of the wall that houses the Reader. e. How system alarms are monitored, for example, from a SCR RMF or ARC. f. The response requirement, and procedures for an alarm at the SAMS level. g. Areas and doors to be controlled and the purpose for applying those controls. h. Performance requirements such as uninterruptible power supply (UPS/battery power for mains failure).

	i. Maintenance requirement and contract arrangements. j. System security measures such as anti-tampering or anti-pass back. k. Responsibility for system audit and frequency. l. Where Dual-factor authentication **MUST** be incorporated, in addition to any token pass that is issued to users. m. Audit trails and logs.
20.4	AACS System Requirements: AACS **MUST** resist attempted attack techniques: a. The specification for AACS **MUST** be in line with government minimum standards. b. AACS products **MUST** be selected based on risk and threat through the Operational Requirements process
20.5	AACS Requirements: a. Processes **MUST** be in place to permit authorised access only. b. Potential attackers **MUST** be prevented from manipulating or disabling the system. c. AACS **MUST** not be accessible from the internet. d. AACS **MUST** be suitably hardened against cyber-attack i.e., protected following CYBER ESSENTIALS, passed CPNI CAPSS (Cyber Assurance Physical Security Systems) testing, NCSC (National Cyber Security Centre) guidance or good commercial cyber protection standards.
20.6	AACS Tokens and Cards **MUST** be: a. Strictly controlled to prevent theft or manipulation. b. Records held of token issue and return for Joiners, Movers, and Leavers.
20.7	Organisations **MUST CONSIDER** the following British Standards at a minimum in the installation of AACS systems: a. **BS EN 60839-11-1:2013** Alarm and electronic security systems. Electronic access control systems. System and components requirements.

	b. **BS EN 60839-11-2:2015** Alarm and electronic security systems. Electronic access control systems. Application guidelines. c. **BS EN 14846:2008** Building hardware. Locks and latches. Electromechanically operated locks and striking plates. Requirements and test methods. d. **BS EN 179:2008** Building hardware. Emergency exit devices operated by a lever handle or push pad, for use on escape routes. Requirements and test methods. e. **BS EN 1125:2008** Building hardware. Panic exit devices operated by a horizontal bar, for use on escape routes. Requirements and test methods. f. **ISO/IEC 7816** Identification cards - Integrated circuit cards. g. **ISO/IEC 15693** Identification cards - Contactless integrated circuit cards, Vicinity cards. h. **ISO/IEC 14443** Identification cards - Contactless integrated circuit cards, Proximity cards.

21. Intruder Detection System and Panic Alarms

Intruder Detection Systems [IDS] are designed to detect the entry, or attempted entry, of an intruder into a protected area, identifying the location of the intrusion and signalling an alarm allowing a response by a guard force or Police. Panic alarms allow the signalling of an alarm to allow guard or Police to respond to the alert.

Reference	
21.1	IDS **MUST** be comprised of the following: a. Control Panel: The Control panel is the brain, and critical component of the Intruder Detection System. b. Sensors: The devices which detect. Sensors are selected based on requirements and environmental conditions. c. Alarm Signalling: Alarm systems commonly use audible and visible warning signals in conjunction with remote signalling to an Alarm Receiving Centre, dependant on response requirements.
21.2	IDS systems are to comply with the latest editions of all relevant standards, codes of practice and statutes that shall include, but not be limited to, the following, where applicable:

	a. All systems **MUST** be installed and maintained to National Security Inspectorate (NSI) Gold • General Data Protection Regulation (GDPR) • Data Protection Act 2018 • Equalities Act 2010 b. PD 6662: 2017 Scheme for the application of European standards for intrusion and hold-up alarm systems. c. NPCC (National Police Chiefs Council) current Alarms Policy or NPCCS (National Police Chiefs Council for Scotland) current Alarms Policy (previously ACPO/S), dependant on premises location.
21.3	The following **MUST** be achieved: a. Coverage over protected areas. b. Use in conjunction with guards to extend coverage into areas not normally accessible to guard patrols for example, roof spaces, external emergency stairs, or locked rooms. c. Integration with other electronic security measures within the site.
21.4	With IDS systems, the following **MUST** be defined: a. The areas, rooms, spaces, doors, windows, and equipment to be protected and the purpose for applying those controls. b. Types of sensors e.g., the ability to identify movement and environmental changes in any defined zones or perimeter that requires protection: • Contact Sensors • Spatial or Volumetric Sensors • Ultrasonic Sensors • Passive Infra-Red Sensors • Microwave Sensors • Beam Interruption Devices • Vibration Sensors • Dual Technology Sensors c. Whether linkage to CCTV is required within the Security Design. d. Any other performance requirements such as UPS. e. Maintenance requirement and / or contract arrangements (Service Level Agreements) (SLAs)).

	f. System security measures such as anti-tampering. g. The detection performance required and how it should be tested (e.g., range and field of view). h. Acceptable false alarm rate (in line with Police unique reference number issue (URN). i. Any special considerations affecting the area(s) concerned and the degree of security. j. Linking to other electronic systems such as CCTV or AACS [integration] as required by the Security Design. k. The overall Site Security Plan and details of all measures (physical and electronic) relevant to the design of the system. l. The type of response force or monitoring arrangements required. m. The location of the alarm display panel and details of related security procedures.
21.5	IDS System Requirements: a. IDS **MUST** be capable of resisting attack techniques. b. The specification for IDS **MUST** be in line with government minimum standards c. IDS products **MUST** be selected based on risk and threat through the Operational Requirements process.
21.6	IDS Installation Requirements: a. Installation **MUST** be in accordance with manufacturers' guidance. b. Physical Security of IDS **MUST** have measures to protect access to cabling power and UPS. c. Processes **MUST** be in place to permit authorised access only. d. Potential attackers **MUS**T be prevented from manipulating or disabling the system, for example, the control system is to be placed in a location that is protected to a level commensurate to the asset you are seeking to protect. e. Use of private networks, while the preferred method of communications for IDS, may be used but appropriate audit logging and security measures **MUST** be applied to prevent un-authorised or un-solicited access via remote connectivity.

	f. Where there are security control panels e.g., alarm control panels, these **MUST NOT** be accessible and operable to members of the public and visitors. g. IDS **MUST** be suitably hardened against cyber-attack i.e., protected following CYBER ESSENTIALS or passed CPNI CAPSS testing or good commercial cyber protection standards.
21.7	Organisations **MUST CONSIDER** the following British Standards at a minimum in the installation of IDS systems: • **BS EN 50131** Alarm systems - Intrusion systems. • **BS 8473** Intruder and hold up alarm systems - Management of false alarms code of practice. • **BS 8243** Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions code of practice.
21.8	Where panic alarms are installed, organisations **MUST CONSIDER** response measures and integration with other systems.

Appendix 1: Enhanced Security Controls

In high threat circumstances, underpinned by the Operational Requirements process and in any Security Risk Assessment or Site Security Plan, enhanced control measures may be required.

22. Hostile Vehicle Mitigation (HVM)

HVM measures are the integration of security processes, procedures and physical obstructions to counter vehicle borne threats.

Reference	
22.1	Organisations **MUST CONSIDER** HVM strategy as an integrated part of the overall protective security process.
22.2	A detailed site-specific security assessment **MUST** be conducted before any HVM countermeasures can be recommended. Details of suitably qualified assessors can be obtained via the Register of Security Engineers and Specialists (RSES) **RSES List.**
22.3	Any HVM installation **MUST** use an impact tested vehicle security barrier (VSB) to standards set in British Standards Institution Publicly Available Specification **BSI PAS 68** or **BSI PAS 170** and be installed with assessments drawn from **BSI PAS 69** (Guidance for installation).
22.4	All works **MUST** comply with: **Anti-Terrorism Traffic Regulation Order** (**ATTRO**) amendments to the **Road Traffic Regulation Act 1984 (England, Scotland & Wales).**

23. Security Control Rooms (SCR)

When the need for a Security Control Room has been identified the standards are defined below. SCRs and their associated physical structure are secure spaces where security operators are stationed to carry out the centralised monitoring and administrative responsibilities of a site's security.

Reference	
23.1	A SCR **MUST** be comprised of the following: a. Secure Room: Large enough to house staff and systems, and **MUST** be located and built-in accordance with

	government standards. b. Electronic Systems: Capabilities and systems **MUST** be selected to provide situational awareness for the operator, with effective displays and monitors. Attention **MUST** be given to environmental conditions, for example overheating. c. Personnel: Effectiveness of the SCR is reliant on the security staff within it. d. Be built in accordance with **ISO 11064 Standard** Ergonomic design of control centres.
23.2	For an effective SCR, the following capabilities **MUST** be provided: a. Systems that provide situational awareness to the operator. b. Better detection ability and positive identification. c. Enable a response to an event or incident. d. Tailored and considered response by security staff. e. Interoperability of multiple electronic systems for example, CCTV can enhance security if used to verify alarms signalled by IDS and AACS. f. Active CCTV monitoring or investigative only. g. IDS, AACS and Panic alarm termination. h. Review recorded CCTV during incidents and alerts. i. Video monitor wall for overview and to inform incident management. j. Telephones, radios, and other communication equipment. k. Body Warn Camera charging and associated network devices and servers. l. Security approved containers, for example key boxes. m. Linkage to centralised SCRs (SECURITY CONTROL ROOM) or supporting RMF. n. Uninterruptable Power Supply (UPS). o. Ability to withstand extreme weather conditions or loss of heating or air conditioning.

	p. Resilience and business continuity. q. Single points of failure.

24. Safe or Refuge Room

Refuge rooms **MUST** be provided where a Security Risk Assessment identifies a high threat of attack for staff or members of the public and its assets.

Reference	
24.1	Refuge Room access **MUST:** a. Be strictly controlled with an automated Access Control System. b. Be used solely for the intended purpose and **MUST NOT** be used as a multi-purpose room, for example, storage or meetings.
24.2	The following **MUST** be conformed with: a. Refuge Rooms to be supported by CCTV and IDS that are capable of being monitored by dedicated security personnel from a Security Control Room (SCR) or Remote Monitoring Facility (RMF). b. Panic alarms to be installed that terminate at a SCR or RMF enabling a security force response. c. Communication equipment to be available to contact Emergency Services. d. Refuge Rooms to allow access to staff-only zones via security doors where possible. e. Refuge Rooms to be designated as a Secure Room; large enough to hold staff and customers in the immediate area based on the building layout. f. Secure Rooms to be built in accordance with **government standards** and in line with CPNI guidance.