LPCB®

Loss Prevention Standard

LPS® 2082 : Issue 1.0

SABRE - Security Assessment Standard For Buildings & Built Infrastructure Assets

bre

CONTENTS **Page**

REVISION OF LOSS PREVENTION STANDARDS

Loss Prevention Standards (LPSs) will be revised by issue of revised editions or amendments. Details will be posted on our website at www.RedBookLive.com.

Technical or other changes which affect the requirements for the approval or certification of the product or service will result in a new issue. Minor or administrative changes (e.g. corrections of spelling and typographical errors, changes to address and copyright details, the addition of notes for clarification etc.) may be made as amendments.

The issue number will be given in decimal format with the integer part giving the issue number and the fractional part giving the number of amendments (e.g. Issue 3.2 indicates that the document is at Issue 3 with 2 amendments).

Users of LPSs should ensure that they possess the latest issue and all amendments.

NOTES

Compliance with this Standard does not confer immunity from legal obligations. Users of LPSs should ensure that they possess the latest issue and all amendments.

BRE Global Limited welcomes comments of a technical or editorial nature on this Standard and these should be addressed to “The SABRE Technical Director” at enquiries@breglobal.co.uk.

BRE and BRE Global Limited are owned by the BRE Trust, which is a registered charity[1]. For further information on our services please contact:

BRE Global Limited
Bucknalls Lane
Garston
Watford
Hertfordshire
WD25 9XX
Telephone: +44 (0)333 321 8811
E-mail: enquiries@breglobal.co.uk
Website: www.bre.co.uk

SABRE is a registered trademark of BRE Global.

FOREWORD

This Standard is applicable to the assessment of buildings and built infrastructure assets and applies to the full life cycle of built assets.

The Standard can be used for sole and shared/multi-occupancy facilities. It identifies technical requirements that are assessed to evaluate the security risk management at a facility and award a facility security assurance rating (SABRE Rating).

Facilities are provided with a SABRE Rating and LPCB certification based on the level of conformity with the technical requirements presented in the Standard. This is demonstrated through the submission of evidence acceptable to BRE Global.

SABRE Rating benchmarks enable facility owners, occupiers and other interested parties to compare one facility with other SABRE rated facilities and a stock of facilities in general.

Full details of the SABRE certification scheme for buildings and built infrastructure assets is provided in Scheme Document SD0229.

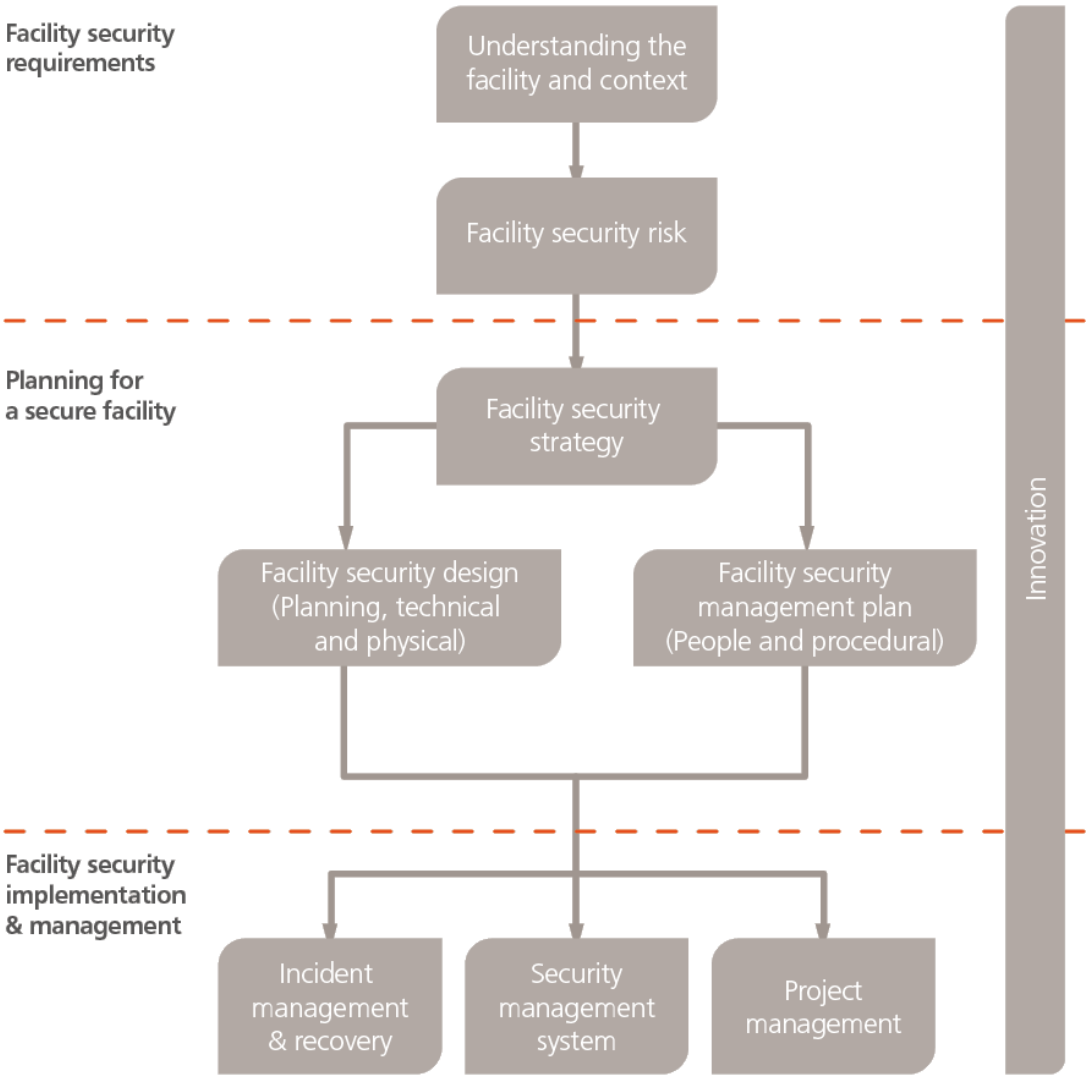
1 SCOPE

This Standard identifies the LPCB technical requirements for rating the security risk management at a facility. The scope includes all types of built assets (buildings and built infrastructure assets) and is relevant to both new and existing (In-Use) facilities.

The Standard includes requirements at each stage in the life cycle of a built asset. It recognises that facility security is influenced by decisions made during pre-planning, planning, design, construction, operation, maintenance, refurbishment/modification and disposal/decommissioning of built assets.

The Standard has been structured and categorised into specific technical sections as illustrated in Figure 1, with each section defining a set of technical aims and associated technical requirements.

Figure 1 SABRE Technical Assessment Structure



Section 1 - Facility Security Requirements

The goal of this section of the Standard is to assess whether management has established and maintained an understanding of their Facility Security Requirements. This understanding directs the planning and management efforts relating to facility security and is fundamental to the achievement of effective facility security.

There are two technical aims in this section:

- **FSR1: The Facility and its Context** encourages the identification of all internal and external issues that will influence facility security.

- **FSR2: Facility Security Risks** encourages the use of security risk assessment to identify priorities for action.

Section 2 - Planning for a Secure Facility

The goal of this section of the Standard is to assess whether management adopt a strategic and holistic approach to the identification and specification of appropriate and proportionate facility security controls.

There are three technical aims in this section:

- **PSF1: Facility Security Strategy** encourages a strategic approach to facility security design and management planning.

- **PSF2: Facility Security Design** encourages the design of environmental, physical and technological controls in accordance with the facility security strategy.

- **PSF3: Facility Security Risk Management Plan** encourages the establishment of personnel and procedural controls that complement the facility security design.

Section 3 - Facility Security Implementation & Management

The goal of this section of the Standard is to assess whether there is strong leadership and commitment to security risk management at a facility. It describes a system for the governance of security at a facility and specific requirements relating to the management of security incidents and changes that will influence a facility and its security.

There are three technical aims in this section:

- **MAN1: Security Risk Management System** encourages the development and operation of a facility level security risk management system that leads to effective security.

- **MAN2: Incident Management & Recovery** encourages a proactive approach to incident management and recovery and the ongoing review of incident performance.

- **MAN3: Project Management** encourages a security minded approach to project management so that change can be used as an opportunity for improvement rather than leading to potential compromises in security.

Innovation in Security Risk Management

The final technical section of the Standard encourages innovation and an aspirational approach to facility security risk management. It gives special recognition to facilities that adopt innovative technology and practices that address previously unresolved security requirements, deliver security performance efficiencies and/or support wider built environment performance objectives.

There is one technical aim in this section:

- **INN1: Innovation** encourages the use of innovative solutions to improve the security performance of a facility.

2 DEFINITIONS

This section defines terms used within this Loss Prevention Standard. Where possible, definitions of common terms were adopted from International, European and British Standards.

Please note that terms may have an alternative definition in law and in other standards, scheme documents or publications produced by BRE Global Limited.

2.1 Adaptability

Ability to change or modify the facility or its systems to maintain security in changing circumstances.

2.2 Adversary

A person or organisation that has the potential to impact the security of another person or organisation.

2.3 Asset

An item, thing or entity that has potential or actual value to an organisation. The value may be derived financially or due to the asset being critical to the organisation's mission.

2.4 Building

A structure that has the provision of shelter for its occupants or contents as one of its main purposes; usually partially or totally enclosed and designed to stand permanently in one place.

2.5 Built Environment

Collection of man-made or inducted physical objects including buildings, other structures, infrastructure and spaces, located in a particular area or region.

2.6 Command & Control

The exercise of authority and direction over assigned resources in the accomplishment of security incident management and recovery.

2.7 Consequence

The outcome of a security incident that has an effect on objectives. Consequences may be categorised as: economic, harm to life, environmental, reputation, compliance and/or mission continuity.

2.8 Construction Works

Everything that is constructed or results from construction operations.

2.9 Convergent Threat

Threat utilising both the physical and cyber domains in order to achieve an adversary's objectives.

2.10 Corporate Security Risk Management

The application of risk management principles in the pursuit of reducing the risks to which an organisation is exposed.

2.11 Cyber Security

A system of controls used to protect an organisation, its facilities and other assets (both physical & cyber) from cyber threats.

2.12 Defence in Depth

A security principle which if adopted will require an adversary to defeat a series of protective layers in sequence to defeat the overall system.

2.13 Dependency

The facility, its security or a security sub-system or component is dependent on another asset or service.

2.14 Design Basis Threat

Derived from a threat assessment, the description of the attributes and characteristics of a credible threat against which a facility and its assets are to be protected.

2.15 Employer

Person or organisation that commissions a project i.e. the construction of a facility or alterations to an existing facility; and is responsible for providing the strategic direction to the professional advisers, contractors and supply chain involved in the planning and implementation of a project.

2.16 Employer Representative(s)

Represents the Employer's security interests during a project at a facility. If appropriate, the role may be fulfilled by the facility Security Manager(s) in the case of in use (existing) facilities.

2.17 Facility

A site and associated assets that is used by its owner for a defined purpose.

2.18 Facility Security Design

The physical and technological controls at the facility.

2.19 Facility Security Risk Management Plan

The proposed personnel and procedural controls required to achieve facility security objectives.

2.20 Facility Security Manager(s)

A role designated by the Responsible Person(s). The role is associated with the necessary Authorities and Responsibilities to ensure facility security objectives can be met.

2.21 Insider

People e.g. staff/contractors; that have either a working knowledge of the organisation and its security controls or who, due to their relationship with the organisation, have authorised access through one or more layers of the organisation's cyber or physical security controls.

2.22 Integrated Design

A holistic approach to the design of a facility that, through the collaboration of many disciplines, leads to better design outcomes.

2.23 Interested Parties

Individual or group that has a vested interest in security decisions and activities at a facility.

2.24 In-Use

An existing facility incorporating one or more buildings or other structures that is used for a defined purpose.

2.25 Intervention

The act or actions of a response force undertaken with the aim of preventing an adversary successfully achieving their objectives and in doing so, preventing or mitigating the losses associated with a security incident.

2.26 Life Cycle

Consecutive and interlinked stages in the life of the facility under consideration.

2.27 Maintenance

Combination of all technical and associated administrative actions during service life, to retain a facility or asset in a state in which it can perform its required functions.

2.28 Modification

A project at an existing facility (In-Use) requiring an assessment/reassessment of facility security. Modifications include refurbishment and end of life activity such as decommissioning or demolition of an existing building or structure at a facility.

2.29 New Facility

The development of a new facility, which excludes projects where construction work is planned at an existing facility (In-Use) e.g. fit-out, refurbishment or modification. Construction works at existing facilities shall be assessed using the In-Use requirements of the Standard.

2.30 Outsider

People that do not have authorised access through one or more layers of an organisation's cyber or physical security controls.

2.31 Performance

Ability to fulfil required functions under intended use conditions or behaviour when in use.

2.32 Personnel Security

A system of controls used to protect an organisation, its facilities and other assets against actions taken by insiders.

2.33 Policy

General commitment, direction, or intention of the Responsible Person(s) with respect to security risk management.

2.34 Procedure

An established/prescribed way of completing an action.

2.35 Process

Series of operations performed to achieve a desired result.

2.36 Product

Item or system manufactured or processed for incorporation in construction works; any goods or service.

2.37 Project

A planned activity, of defined duration, undertaken to achieve a specific goal and resulting in a change to the facility security needs or existing security function. Examples include:

- Facility, building or asset disposal e.g. change of ownership or occupation
- Facility modification/alteration involving construction work(s)
- Demolition (End of Life)
- Change of use

2.38 Project Security Manager(s)

A role within the project team designated by the Employer Representative(s), with the holder being responsible and accountable for compliance with the project security brief.

2.39 Recovery

Return to normal operations following a security incident and completion of response actions.

2.40 Resilience

Ability to maintain and adapt in response to changing circumstances, including changes in security threat, facility operations, maintenance and sub-system failures.

2.41 Response

The act or actions following the detection and confirmation of a security incident/breach.

2.42 Responsible Person(s) [1]

The person(s) holding ultimate responsibility for facility security. They can be identified as:

- the person(s) in control of the facility (as occupier or otherwise) in connection with the carrying on by him of a trade, business or other undertaking (for profit or not); or
- the owner(s), where the person(s) in control of the premises does not have control in connection with the carrying on by that person of a trade, business or other undertaking.

2.43 Physical Security

A system of controls used to protect an organisation, its facilities and other assets (physical and cyber) from physical threats.

2.44 Risk

Effect of uncertainty on objectives.

2.45 Risk Assessment

The process of identifying, analysing and evaluating security risk.

2.46 Risk Criteria

Terms of reference used to evaluate the significance or importance of an organisation's risks. They are used to determine whether a specified level of risk is tolerable or intolerable.

2.47 Scalability

Ability to change or modify a facility, its systems or sub-systems to escalate or de-escalate security controls in response to changing security threat.

---

[1] For a facility occupied by a single organisation (user), it will be relatively straightforward to identify the responsible person(s). However, in the case of shared facilities, there are likely to be multiple Responsible Persons.

2.48 Security

State of being free from harm or fear of criminal activity.

2.49 Security Manager(s)

A security role appointed by the Responsible Person(s) or Employer Representative(s).

2.50 Security Risk

The likelihood that a threat will be realised, together with a measure of the potential consequences associated with the realisation of the threat.

2.51 Security Risk Management

Activities conducted to direct and control security risk(s).

2.52 Security Risk Management System

An organised, systematic approach to managing security risks which embeds security into the culture and day-to-day activities at a facility.

2.53 Significant Finding(s)

Risks that are important and warrant further attention as they exceed the facility risk criteria.

2.54 Site

Area of land under defined ownership on which a facility is constructed.

2.55 Threat[2]

Statement or intention to inflict pain, injury, damage, or other hostile action to an organisation, a facility or assets.

2.56 User

Person or organisation for which a facility is designed or that makes use of a facility during its life (including the building owner, manager and occupants).

2.57 Vulnerability

A weakness to a security threat which reduces the security of a facility.

[2] A threat may originate externally to an organisation (outsider threat) or from within (insider threat).

3 REQUIREMENTS

3.1 Evidence Requirements

SABRE is a third party assessment and certification scheme. The scheme is operated in a consistent and reliable manner and this provides confidence in the assessment ratings determined by the SABRE Assessors.

The SABRE Assessor determines the SABRE Rating and their assessment report is the formal record of the facility audit against the technical requirements outlined in this Standard.

The audit requires the certification applicant to share information relating to their facility and its security with the SABRE Assessor in order to facilitate assessment and certification. To maintain consistency, all certification decisions shall be based on verified and credible information that is traceable i.e. evidence based.

Evidence principles and a detailed commentary on the process of gathering evidence relating to a facility, its use in facility security assessment and for benchmarking purposes is provided in Scheme Document SD0229.

3.2 Technical Requirements

3.2.1 Section 1 - Facility Security Requirements Section

The requirements in this section encourage the Responsible Person(s) and their nominated Facility Security Manager(s) to establish and maintain an understanding of their facility security requirements and facility security risks, and in doing so allow:

- development of appropriate security objectives;
- informed decisions to be made in relation to facility risk(s); and
- consideration of strategic options for mitigating these risks.

CORE TECHNICAL STANDARD AIM	
FSR 1: The Facility & Its Context *To recognise and encourage the identification of internal and external issues that are relevant to the purpose of the facility and influence its security risk management objectives.*	
CORE TECHNICAL STANDARD REQUIREMENTS	
FSR 1.1: Facility Attributes & Setting	
New Facility In-Use	**(A)** The Security Manager(s) shall take into account the following external and internal factors when determining facility security objectives: • Use, functions and supporting activities. • Modes of operation. • Facility context i.e. location and setting. • Users/User Groups. • Site security constraints.
FSR 1.2 Interested Parties	
New Facility In-Use	**(A)** The Security Manager(s) shall demonstrate an understanding of the needs and expectations of interested parties, including: • users; • local authorities; • regulators and law enforcement entities; • neighbours and the wider community; • landlord, tenants and fellow tenants; • insurers; • investors; and • customers and suppliers.

FSR 1.3 Corporate Security Risk Management Requirements	
New Facility In-Use	**(A)** The Security Manager(s) shall determine any corporate security risk management requirements when establishing facility security objectives.
FSR 1.4 Legal and Regulatory Requirements	
New Facility	**(A)** The Security Manager(s) shall determine and take into account the legal and regulatory requirements relating to the facility, its function, activities and services when establishing facility security objectives. *Note: Factors that influence security requirements are likely to include, but not be limited to, privacy, fire safety, health & safety and equality & diversity.*
In-Use	**(A)** The Security Manager(s) shall define, document, implement and maintain procedures to determine the legal and regulatory requirements relating to the facility, its function, activities and services. **(B)** The Security Manager(s) shall take these requirements into account when establishing facility security objectives. *Note: Factors that influence security requirements are likely to include, but not be limited to, privacy, fire safety, health & safety and equality & diversity.*
FSR 1.5 Security Dependencies	
New Facility In-Use	**(A)** The Security Manager(s) shall identify services upon which the security of the facility is dependent and take these into account when conducting security risk assessment. *Note 1: Examples may or may not include assumed or pre-determined service level agreements and attendance arrangements with 3rd parties, such as:* • *energy suppliers;* • *water suppliers;* • *communication and alarm response providers;* • *contracted security service providers; and* • *emergency services.* *Note 2: Assessment of facility dependencies will allow resilience to be built into the facility security strategy.*

FSR 1.6 Asset Identification & Valuation	
New Facility In-Use	**(A)** The Security Manager(s) shall identify facility user(s) assets and those of relevant interested parties. **(B)** The Security Manager(s) shall conduct a value assessment to identify critical assets that shall be taken into account when conducting security risk assessment. *Note 1: Asset categories for valuation purposes shall include:* • *physical assets;* • *people;* • *information assets; and* • *facility services.* *Note 2: Value assessment criteria may or may not include:* • *Relative Value (monetary £/$);* • *Recovery time following loss, damage or destruction (time);* • *Non-compliance (financial claims, prosecutions, loss of franchise/licence); or* • *Reputation (goodwill): media coverage (duration and extent), reduction in sales (£/$), terminated contracts (£/$).*
FSR 1.7 Facility Security Risk Management Objectives	
New Facility	**(A)** Project security objectives shall be established that: 1. take into account applicable requirements determined in **FSR1.1-1.6**; 2. are measurable to allow performance to be evaluated; and 3. are presented within the project security brief so that design quality and project success (outcomes) can be evaluated.

In-Use	**(A)** The Security Manager(s) shall establish facility security objectives that are consistent with, and support the facility security policy. **(B)** The security objectives shall: • be measurable to allow performance to be evaluated; and • take into account applicable requirements determined in **FSR1.1-1.6**. **(C)** Objectives shall be: • monitored; • communicated; and • reviewed at planned intervals and updated as appropriate. *Note: Objectives are not static and need to be updated in view of the security climate, the expectations of interested parties and continual improvement activities. Objectives can be revised up or down but the most important thing is to ensure that any changes are communicated.*

CORE TECHNICAL STANDARD AIM	
FSR 2: Facility Security Risks *To recognise and encourage the adoption of security risk assessment as the means of establishing facility security priorities and informing the strategic approach to enhancing facility security performance.*	
CORE TECHNICAL STANDARD REQUIREMENTS	
FSR 2.1 Security Risk Assessment	
New Facility In-Use	**(A)** The Security Manager(s) shall adopt security risk assessment as the basis for determining facility security function priorities. **(B)** Security risks shall be determined through the assessment of credible threats, facility vulnerabilities to those threats and associated consequences. **(C)** Risks shall be: • monitored; • communicated; • reviewed at planned intervals; and • updated as appropriate.
FSR 2.2 Threat Assessment (T)	
New Facility In-Use	**(A)** The Security Manager(s) shall undertake a threat assessment, drawing on internal and external sources of information to identify credible security threats to the facility. **(B)** The threat assessment shall be conducted in consultation with interested parties. **(C)** The threat assessment shall take account of how the following factors related to the facility influence security threat: 1. Use, functions and supporting activities 2. Context e.g. location, setting 3. Users/user groups 4. Owner 5. Planning and design

	(D) The scope of the threat assessment shall extend, as appropriate, to: • outsider and insider threats; • cyber, physical and convergent threats; and • threats against the facility itself and information relating to the facility and its security. **(E)** The findings of the threat assessment shall be articulated into credible Design Basis Threat (DBTs) and documented.
FSR 2.3 Vulnerability Assessment (V)	
New Facility In-Use	**(A)** The Security Manager(s) shall assess the vulnerabilities of the facility having regard for credible threats determined in **FSR2.2A.** **(B)** A vulnerability shall be reported where assessment indicates the facility security system may not result in threat intervention and neutralisation prior to losses being incurred.
FSR 2.4 Consequence Assessment (C)	
New Facility In-Use	**(A)** The Security Manager(s) shall assess security incident consequences based on the credible threats determined in **FSR2.2A.** **(B)** Consequences shall be graded in terms of severity and duration. *Note: Potential consequences may extend, but not be limited to, loss of asset value, mission disruption, non-compliance, reputational and environmental damage.*
FSR 2.5 Risk Evaluation	
New Facility	**(A)** Risks shall be evaluated against risk criteria pre-agreed in the project brief or in the absence of pre-defined criteria, shall be communicated to the project Employer Representative(s) for approval. *Note: In the case of speculative development projects, where the end user is unknown, it is important for all parties involved in the development process, including those providing security recommendations, to have well defined objectives which can be*

	used for evaluating whether development proposals meet the employer requirement.
In-Use	**(A)** Risks shall be evaluated against risk criteria. Criteria shall be pre-agreed with the Responsible Person(s) or in the absence of pre-defined criteria, shall be communicated to the Responsible Person(s) for approval.
FSR 2.6 Strategic Options Appraisal	
New Facility	**(A)** The Security Manager(s) shall appraise strategic risk mitigation options to address significant findings**.** **(B)** Appraisal shall include the following strategic options: • Avoiding the risk by deciding not to start or continue with the activity; • Taking or increasing the risk in order to pursue an opportunity; • Removing the source of the risk; • Changing the likelihood; • Changing the consequences; • Sharing the risk with another party or parties; and • Retaining the risk by informed decision.
In-Use	
FSR 2.7 Risk Communication & Documentation	
New Facility	**(A)** The Security Manager(s) shall communicate the significant findings of the security risk assessment to the Employer's Representative(s) for approval, including strategic recommendations for risk mitigation (if appropriate) and any residual risks.
In-Use	**(A)** The Security Manager(s) shall communicate the significant findings of the risk assessment to the Responsible Person(s) for approval, including strategic recommendations of risk mitigation (as appropriate) and any residual risks.

3.2.2 Section 2 - Planning for a Secure Facility

The requirements in this section encourage:

- adoption of a strategic approach to the planning and design of facility security controls;
- appropriate balance between security design elements e.g. physical and technological security controls; and management e.g. personnel and procedural controls;
- application of security risk management principles which have in mind the ultimate facility security objectives;
- documentation and communication of management expectations at an early stage in the development of new construction projects;
- integrated design to ensure solutions are fit for purpose.

CORE TECHNICAL STANDARD AIM	
PSF 1: Facility Security Strategy *To recognise and encourage the development of a holistic facility security strategy that draws on design of a facility and its management to mitigate credible security risks and achieve the facility security objectives.*	
CORE TECHNICAL STANDARD REQUIREMENTS	
PSF 1.1 A Holistic Approach	
New Facility	**(A)** The project Security Manager(s) shall develop a holistic security strategy for the facility. **(B)** The strategy shall make use of security-minded facility planning (physical environment) and the deployment of personnel, technological, physical and procedural controls to mitigate the highest priority security risks in accordance with the facility security objectives **(FSR1.7).** **(C)** The strategy shall outline the performance requirements of controls in relation to the primary security functions they perform, specifically: • **Disrupt or Deny** an attack on a facility through deployment of security controls that reduce the consequences of an adversary attack • **Deter** an attack by reducing facility target attractiveness. This will require the adversary to perceive a lower likelihood of success, higher level of effort for a similar or lesser gain and/or increased likelihood of response intervention. • **Detect** an attack should one be launched so that a timely and effective response may be initiated • **Delay** an attack for a sufficient time to allow appropriate on-site and off-site response to be initiated • **Respond** before the adversary completes an attack in order to reduce incident consequences • **Recover** from an attack/security breach at the facility and return to normal operations

In-Use	**(A)** The facility Security Manager(s) shall develop a holistic security strategy for facility security risk management. **(B)** The strategy shall make use of security-minded facility planning (physical environment) and the deployment of personnel, technological, physical and procedural controls to mitigate the highest priority security risks in accordance with facility security objectives **(FSR1.7).** **(C)** The strategy shall outline the performance requirements of controls in relation to the primary security functions they perform, specifically: • **Disrupt or Deny** an attack on a facility through deployment of security controls and in doing so reduce the consequences of an adversary attack • **Deter** an attack by reducing facility target attractiveness. This will require the adversary to perceive a lower likelihood of success, higher level of effort for a similar or lesser gain and/or increased likelihood of response intervention. • **Detect** an attack should one be launched so that a timely and effective response may be initiated • **Delay** an attack for a sufficient time to allow appropriate on-site and off-site response • **Respond** to an attack to prevent adversary success and/or facilitate incident response actions that reduce incident consequences • **Recover** from an attack/security breach at the facility and return to normal operations
PSF 1.2 A 'Systems' Approach	
New Facility	**(A)** The facility security strategy shall ensure individual security controls are integrated and interoperable to the extent required to achieve the facility security objectives.
In-Use	

PSF 1.3 Fit for Purpose	
New Facility In-Use	**(A)** The facility security strategy shall accommodate end user objectives and engender the support of interested parties during its implementation.
PSF 1.4 Layering and Defence in Depth	
New Facility In-Use	**(A)** The facility security strategy shall ensure that in order for an adversary to defeat the facility security system, they will need to defeat successive protection layers. **(B)** The facility security strategy shall incorporate a range of diverse security controls.
PSF 1.5 Resilience (Adaptability & Scalability)	
New Facility In-Use	**(A)** The facility security strategy shall demonstrate adaptability and scalability, ensuring that security can be maintained in the following circumstances: • Changing security threat. • Different facility operating modes. • Systems maintenance. • System and component failures. *Note: The method(s) of evidencing appropriate facility security resilience will be dependent on the type of facility, its security requirements and the proposed facility security strategy. Methods might include the development of simple 'what if?' scenarios, Fault Tree Analysis (FTA) and/or Event Tree Analysis (ETA).*
PSF 1.6 Balanced Protection	
New Facility In-Use	**(A)** The facility security strategy shall ensure an adversary will encounter security controls regardless of how they attempt to defeat the system.
PSF 1.7 Security Strategy Communication	
New Facility	**(A)** The project Security Manager(s) shall communicate the facility security strategy to the Employer's Representative(s) for approval.
In-Use	**(A)** The facility Security Manager(s) shall communicate the facility security strategy to the Responsible Person(s) for approval.

CORE TECHNICAL STANDARD AIM	
PSF 2: Facility Security Design *To recognise and reward a facility security design that integrates a series of environmental, physical and technological controls in accordance with the facility security strategy.*	
CORE TECHNICAL STANDARD REQUIREMENTS	
PSF 2.1 Physical & Technical Design	
New Facility In-Use	**(A)** The facility security design shall be in accordance with the facility security strategy and detail the physical and technical controls that support overall facility security. *Note: Security controls may or may not include the following:* • *control and monitoring equipment;* • *communication systems;* • *access control;* • *lighting;* • *intruder detection systems;* • *personal protection systems and equipment; and* • *passive and active barriers e.g. walls, fences, doors, windows, safes and secure storage, hostile vehicle mitigation.*
PSF 2.2 Integrated Security Design	
New Facility In-Use	**(A)** The facility security design shall be fully coordinated with other design elements of the facility. *Note: For example, the security design should not inhibit facility accessibility for legitimate users and the security design must be coordinated to ensure compliance with health & safety and fire safety requirements.*
PSF 2.3 Designed with Maintenance in Mind	
New Facility In-Use	**(A)** The facility shall be designed to minimise any negative effects of maintenance activities on security.

CORE TECHNICAL STANDARD AIM	
PSF 3: Facility Security Risk Management Plan *To recognise and reward the identification, documentation and communication of the management plan (personnel and procedural security controls) required in support of the facility security design to successfully implement the facility security strategy.*	
CORE TECHNICAL STANDARD REQUIREMENTS	
PSF 3.1 People and Procedures	
New Facility	**(A)** The project Security Manager(s) shall develop and document a facility security risk management plan / Concept of Operations (CONOPs). **(B)** The plan shall detail management aspects (personnel and procedural controls) necessary to support successful implementation of the facility security strategy. *Note: Any assumptions relating to support provided by 3rd parties should be documented in the plan to ensure that end users have a clear understanding of their role and the role of others in the delivery of effective facility security.*
In-Use	**(A)** The facility Security Manager(s) shall develop, document and maintain a facility security risk management plan / Concept of Operations (CONOPs) that is in accordance with the requirements of the facility security strategy. **(B)** The plan shall detail management aspects (personnel and procedural controls) necessary to support successful implementation of the facility security strategy. **(C)** The plan shall document the role of 3rd parties in the delivery of effective facility security.
PSF 3.2 Security Organisation	
New Facility	**(A)** The facility security risk management plan shall outline the security organisation structure for the facility. **(B)** The security organisation shall include a suitable number of persons to implement the facility security strategy.
In-Use	

PSF 3.3 Roles & Responsibilities	
New Facility	**(A)** The facility security risk management plan shall outline the responsibilities of each role within the facility security organisation.
In-Use	
PSF 3.4 Competence	
New Facility	**(A)** The facility security risk management plan shall outline the competencies required for each role within the security organisation.
In-Use	

3.2.3 Section 3 - Facility Security Implementation & Management

The requirements in this section encourage:

- leadership and commitment to facility security;
- the operation and maintenance of an effective security risk management system;
- a proactive approach to incident management, recovery and post incident review; and
- a security minded approach to managing change that influences security requirements, security plans and management.

Notes:

1) The requirements relating to Security Risk Management System (MAN1) and Incident Management & Recovery (MAN2) are applicable only to existing facilities (In-Use) and do not form part of the assessment of new facilities.

2) The requirements relating to Project Management (MAN3) are applicable to both new facilities and existing facilities (In-Use) that have undergone change which has influenced facility security requirements, facility security planning and/or the management of security.

CORE TECHNICAL STANDARD AIM	
MAN 1: Security Risk Management System (SRMS) *Recognise and reward the establishment and operation of a facility-level security risk management system that supports the implementation of effective facility security*	
CORE TECHNICAL STANDARD REQUIREMENTS	
MAN 1.1 Security Leadership	
New Facility	N/A
In-Use	**(A)** The Responsible Person(s) at the facility shall demonstrate leadership and commitment to security risk management by: 1. designating a Security Manager(s) for facility security; 2. ensuring the establishment of security risk management policy and objectives;

	3. ensuring integration of security risk management requirements within the organisation's business processes; 4. budgeting for facility security risk management; 5. communicating the importance of security risk management at the facility; 6. monitoring and evaluating performance of the security management system; and 7. seeking and promoting continual improvement.

MAN 1.2 Security Policy	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) at the facility shall establish a facility security policy. **(B)** The facility security policy shall: 1. be suitable given the type of facility and its context **(FSR1)**; 2. be complementary to other relevant policies; 3. include a commitment to meet applicable requirements; 4. include a commitment to prioritise resources at the highest security risks; 5. include a commitment to manage risks to an appropriate and proportionate level (**FSR 2**); 6. include a commitment to continual improvement (**MAN 1.17**); 7. be available as documented information; 8. be communicated and understood by persons conducting work under the control of the facility Responsible Person(s); 9. be available to interested parties (as appropriate); and 10. reviewed at planned intervals. **(C)** The Security Manager(s) shall sign and seek approval of the policy by the Responsible Person(s). **(D)** The Security Manager(s) shall implement the facility security policy on behalf of the Responsible Person(s).
MAN 1.3: Security Roles, Responsibilities & Authority	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall be accountable to the Responsible Person(s) for security risk management at the facility and reporting on performance, including making recommendations for improvement.

	(B) The Security Manager(s) shall have authority to implement the facility security policy on behalf of the Responsible Person(s). **(C)** The Security Manager(s) shall assign all other roles within the facility security organisation based on the facility security management responsibility, authority and competence requirements. **(D)** The Security Manager(s) shall communicate the security risk management responsibilities (including regulatory obligations) of personnel, tenants and 3rd parties who do not have defined security roles at the facility.
MAN 1.4 Cooperation & Coordination	
New Facility	N/A
In-Use	**(A)** Where two or more organisations share or have responsibilities in respect of a facility (whether on a temporary or a permanent basis) each such person shall be regarded as a Responsible Person and shall: 1. Co-operate with the other Responsible Person(s) concerned, so far as is necessary to enable them to comply with the requirements of this Standard. 2. Take all reasonable steps to inform the other Responsible Person(s) of the security risks relevant to the security of the facility as a whole, arising out of or in connection with their activities/use of the facility. 3. Establish and comply with the requirements of a Responsible Person(s) working agreement. The agreement shall provide effective security leadership for the facility, including the establishment of a mechanism, such as a Facility Security Committee, which discharges the security leadership requirements of this standard on behalf of all Responsible Persons.
MAN 1.5 Facility Security Strategy	
New Facility	N/A

In-Use	**(A)** The Security Manager(s) shall establish a security strategy procedure for the facility. The procedure shall: • ensure the documentation and maintenance of a facility security strategy; • document roles and responsibilities for strategy development, documentation and maintenance; • require communication of the security strategy to the Responsible Person(s) for review and approval.
Man 1.6 Resources/Support	
New Facility	N/A
In-Use	**(A)** The Responsible Person(s) shall allocate capital and operational resources adequate to comply with facility security policy and objectives.
MAN 1.7 Competence	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall be responsible for: 1. acquiring and maintaining competence for the role on the basis of skills, knowledge, qualifications and/or experience; 2. taking actions to acquire new competencies, and evaluating the effectiveness of the actions taken; and 3. retaining documented information as evidence of competence. **(B)** The Security Manager(s) shall be responsible for: 1. ensuring that the persons conducting work under the control of the Responsible Person(s) or that affect facility security are competent on the basis of their skills, knowledge, qualifications and/or experience; 2. where applicable, taking actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and 3. retaining appropriate documented information as evidence of competence.

MAN 1.8 Training & Exercises (Drills)	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall identify, document and maintain training policies and procedures that ensure facility personnel with security responsibilities receive appropriate training in accordance with competency requirements. **(B)** The Security Manager(s) shall plan, conduct, document and maintain records of incident drills in order to test the effectiveness of facility security. *Note: Drills may be conducted as table top exercises or in the field. In the case of the latter, the documentation produced by the Security Manager(s) shall include the objectives of the field exercise and why these could not be achieved through other methods associated with lower operational and safety risks e.g. table top exercise or virtual reality simulation.* *The benefits of such exercises should be assessed against the costs and risks. If such exercises are undertaken, suitable controls should be implemented to manage these risks.*
MAN 1.9 Security Awareness & Communication	
New Facility	N/A
In-Use	**(A)** Persons doing work under the control of the facility management shall be aware of: 1. the facility security policy; 2. their contribution to facility security, 3. the benefits of effective facility security; 4. the implications of not conforming with security policy and associated requirements; and 5. the security risks to them arising from or in connection with their use of the facility and their work.

MAN 1.10 Documented Information	
New Facility	N/A
In-Use	**(A)** The Security Risk Management System (SRMS) shall include documented information: 1. required by this Standard; and 2. determined by the organisation as being necessary for the effectiveness of the SRMS.
MAN 1.11 Testing, Commissioning, Maintenance & Repair	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall plan, document, implement and control the processes for maintenance, testing and repair of security systems to ensure: 1. that they operate correctly in the event of a security incident; 2. optimum performance and reduced system or sub-system(s) downtime. **(B)** Security systems (physical and technological) shall be subject to re-commissioning and/or continuous commissioning as appropriate. This shall include seasonal commissioning where necessary to validate the performance of systems under all operational conditions.
MAN 1.12 Facility Information Security	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall establish, document and implement the policies, procedures, technological and physical controls necessary to protect information relating to the facility and its security throughout the life of the facility.

Man 1.13 Performance Monitoring & Evaluation	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall establish procedures for monitoring and evaluating facility security performance; and the effectiveness of the security risk management system. **(B)** The Security Manager(s) shall establish: 1. what needs to be monitored and measured; 2. the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; 3. when the monitoring and measuring shall be performed; 4. periods of re-evaluation at planned intervals to satisfy the monitoring and measuring requirements. **(C)** The requirements shall be agreed and approved by the Responsible Person(s). **(D)** The Security Manager(s) shall retain appropriate documented information as evidence of the monitoring and evaluation results.
Man 1.14 Audit	
New Facility	N/A
In-Use	**(A)** The Responsible Person(s) shall conduct audits at planned intervals to provide information on whether the security risk management system: 1. conforms with the requirements of this standard; and 2. is effectively implemented and maintained. **(B)** The Responsible Person(s) shall establish, implement, maintain and document an audit programme and select auditors to ensure the impartiality and objectivity of the audit process.

MAN 1.15 Management Review	
New Facility	N/A
In-Use	**(A)** The Responsible Person(s) shall review the facility's SRMS at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. **(B)** Management review shall include: 1. changes to the facility and its context; 2. changes to the facility security risks; 3. status of actions from previous management reviews; 4. facility security performance; and 5. audit results related to the SRMS. **(C)** The Responsible Person(s) shall identify: 1. opportunities for improvements that will offer enhanced security/SRMS performance; 2. and allocate additional resources if appropriate in support of making improvements; and 3. changes to the SRMS if appropriate. **(D)** The Responsible Person(s) shall document and maintain records of the management reviews.
MAN 1.16 Non Conformity & Corrective Actions	
New Facility	N/A
In-Use	**(A)** When a non-conformity occurs, the Security Manager(s) shall take actions to control and correct the issue and manage the consequences of the non-conformity. **(B)** The Security Manager(s) shall determine whether actions are required to eliminate the causes of the nonconformity to prevent or reduce the likelihood of reoccurrence. This will include: 1. reviewing the nonconformity; 2. identifying the causes of the nonconformity.

	(C) The Responsible Person(s) shall give the Security Manager(s) authority to: 1. implement appropriate actions; 2. review the effectiveness of such corrective actions; and 3. make changes to the SRMS if necessary. **(D)** The Security Manager(s) shall retain records as evidence of nonconformities and any subsequent actions taken; and the results of any corrective action.
MAN 1.17 Continual Improvement	
New Facility	N/A
In-Use	**(A)** The Responsible Person(s) shall continually improve the suitability, adequacy and effectiveness of the SRMS.

CORE TECHNICAL STANDARD AIM	
MAN 2: Incident Management & Recovery *Recognise and encourage management practices that lead to timely incident identification, effective incident response and the evaluation of incident performance to reduce the likelihood and consequences of future occurrence(s).*	
CORE TECHNICAL STANDARD REQUIREMENTS	
MAN 2.1 Security Incident Detection and Communication	
New Facility	N/A
In-Use	**(A)** The facility Security Manager(s) shall establish, document and maintain procedures for identifying and communicating a security incident or emergency, including means of communicating: 1. with the Responsible Person(s); 2. with those having facility security responsibilities; 3. to occupants that have no defined security duties; 4. with the emergency services; 5. with those contracted to provide services that will influence incident outcomes; 6. with other interested parties as appropriate.
MAN 2.2: Threat Communication	
New Facility	N/A
In-Use	**(A)** The facility Security Manager(s) shall establish, document and maintain procedures for communicating changes in security threat. *Note: Threat level may be established from one or more of the following:* *1. intelligence relating to the facility;* *2. receipt of a threat directed at the facility or its users;* *3. changes in national, regional or sector security threat;*

	4. changes in the threat to the end user organisation; *5. a publically broadcast incident at a comparable facility or organisation; and* *6. receipt of advice from a national security advisory system, the security services, regulator or law enforcement body.*
MAN 2.3: Incident Command & Control	
New Facility	N/A
In-Use	**(A)** The facility Security Manager(s) shall establish and operate an incident management structure at the facility.
MAN 2.4: Incident Intervention & Response Actions	
New Facility	N/A
In-Use	**(A)** The facility Security Manager(s) shall establish, document and maintain procedures for incident intervention & response actions. *Note: Response actions may or may not include:* *1. protection of critical assets;* *2. actions to protect human life (e.g. evacuation);* *3. threat neutralisation* *4. containment and stabilisation of the incident.*
MAN 2.5 Recovery Actions	
New Facility	N/A
In-Use	**(A)** The facility Security Manager(s) shall establish, document and maintain procedures for incident recovery. *Note: Recovery actions may or may not include:* *1. re-occupation of the facility;* *2. replacement of lost stock or raw materials;* *3. re-establishing utilities (power, communications)* *4. re-establishing critical corporate functions.*

MAN 2.6 Incident Performance - Monitoring & Evaluation	
New Facility	N/A
In-Use	**(A)** The Security Manager(s) shall establish a procedure(s) for monitoring and evaluating incident management performance. **(B)** Performance shall be reported to the Responsible Person(s) following major incidents and at periodic intervals as appropriate. **(C)** The Security Manager(s) shall retain appropriate documented information as evidence of the results.

CORE TECHNICAL STANDARD AIM	
MAN 3: Project Management *Recognise and encourage project management, design and procurement practices that optimise facility security performance and design quality.*	
CORE TECHNICAL STANDARD REQUIREMENTS	
MAN 3.1 Project Leadership	
New Facility In-Use	**(A)** The Responsible Person(s) shall demonstrate leadership and commitment to security risk management by: 1. designating for a project, an Employer Representative(s) for security; 2. ensuring a security budget is available for projects; and 3. communicating to the project team and interested parties, the importance of security as a criteria in judging the success of a project. *Note: For projects undertaken at existing facilities and dependent on the type, duration and scale of the project being undertaken, the role of Employer Representative(s) may be fulfilled by the facility Security Manager(s) if appropriate.*
MAN 3.2 Security Roles, Responsibilities & Authority	
New Facility In-Use	**(A)** The Employer Representative(s) shall: 1. represent the interests of the Responsible Person(s) and ensure a project meets the employer's security objectives set out in the project brief; 2. designate a project 'Security Manager(s)' within the project team; and 3. review and approve all project information exchanges required by this standard, prior to authorising further project development.

	(B) The project Security Manager(s) shall be: **1.** accountable to the Employer Representative(s) for all aspects of project security; **2.** responsible for identifying and assigning roles, responsibilities and authorities to all personnel, contractors and suppliers employer directly or indirectly to contribute to the delivery of a project; and **3.** responsible for delivery of a project in compliance with the security objectives outlined in the project brief.
MAN 3.3 Employer Information Security Requirements	
New Facility In Use	**(A)** The Employer Representative(s) shall: 1. document Employer Information Security Requirements (EISRs) for projects undertaken at the facility; 2. communicate the importance of compliance with the EISRs; 3. monitor compliance with EISRs and take corrective actions in the event on non-compliance. *Note: For projects involving demolition, change of use or occupier, the EISRs should identify any information assets:* *1. to be retained by the Employer;* *2. requiring destruction, disposal or desensitisation and any specific requirements related to this process; and* *3. to be handed over to the new owner/occupier (if applicable).*

MAN 3.4 Project Security Brief	
New Facility	**(A)** The Employer Representative shall ensure the documentation of a project security risk assessment in accordance with **FSR2.1(A2)**. **(B)** The Employer Representative(s) shall ensure the development, documentation and maintenance of a security brief for the project. *Metric(s):* Evidence of the above in executed projects.
In Use	**(A)** The Employer Representative shall ensure the documentation of a project security risk assessment which shall be updated, as a minimum, at each project milestone. **(B)** The project security risk assessment shall: 1. identify any new security risks as a result of the project. 2. the influence of the project (positive / negative / none) on the existing facility security risks. 3. identify temporary risks associated with project implementation stage **(C)** The Employer Representative(s) shall ensure the development, documentation and maintenance of a security brief for the project. **(D)** The project security brief shall outline any employer requirements / constraints relating to the procurement of security products and services, including any known interoperability requirements associated with existing systems.
MAN 3.5 Project Security Strategy	
New Facility	**(A)** The project Security Manager(s) shall develop, document and communicate a project security strategy in accordance with **PSF 1.1**.
In Use	**(A)** The project Security Manager(s) shall develop, document and communicate a project security strategy.

	(B) The project security strategy shall make use of security-minded facility planning (physical environment) and the deployment of personnel, technological, physical and procedural controls to mitigate the highest priority security risks in accordance with the facility security objectives (**FSR1.7**). **(C)** The project security strategy shall outline the performance requirements of controls in relation to the primary security functions they perform, specifically: • **Disrupt or Deny** an attack on a facility through deployment of security controls and in doing so reduce the consequences of an adversary attack • **Deter** an attack by reducing facility target attractiveness. This will require the adversary to perceive a lower likelihood of success, higher level of effort for a similar or lesser gain and/or increased likelihood of response intervention. • **Detect** an attack should one be launched so that a timely and effective response may be initiated • **Delay** an attack for a sufficient time to allow appropriate on-site and off-site response • **Respond** to an attack to prevent adversary success and/or facilitate incident response actions that reduce incident consequences • **Recover** from an attack/security breach at the facility and return to normal operations **(D)** The project security strategy shall be coordinated with the existing facility strategy in order to ensure compliance with the interoperability requirements documented in the project brief.

MAN 3.6 Project Security Design	
New Facility In Use	**(A)** The project Security Manager(s) shall develop, document and communicate the project security design in accordance with **PSF2.1.** **(B)** The design shall be developed in accordance with the project contract and associated project programme, with information exchanges providing an appropriate Level of Detail (LOD) at each project stage to allow: 1) effective design coordination with other design disciplines; 2) cost information to be prepared for budgeting purposes and project financial performance evaluation; 3) successful project contract tendering and award; and 4) design review and approval by the Employer Representative(s).
MAN 3.7 Project Security Risk Management Plan	
New Facility	**(A)** The project Security Manager(s) shall develop, and document a project security risk management plan in accordance with the requirements of **PSF3.1.**
In Use	**(A)** The project Security Manager(s) shall develop, and document a project security risk management plan in accordance with the requirements of **PSF3.1.**
MAN 3.8 Procurement of Security Products & Services	
New Facility In Use	**(A)** The procurement of security products and services shall be in accordance with any requirements outlined in the Project Brief and the project security design.

	Note: Requirements set out in the project brief may or may not include: 1) *product testing, certification and inspection, including restrictions on the procurement of products that do not meet industry best practice and recognised standards, are not 3rd party tested and certified; and* 2) *supply chain competency assessment and vetting, including restrictions on the procurement of services that do not meet industry standards and best practice and that are not 3rd party licensed or certified.*
MAN 3.9 Project Handover Strategy	
New Facility In Use	**(A)** The project Security Manager(s) shall establish, document, maintain and communicate a handover strategy for the project. **(B)** The handover strategy shall be made available as part of tender documentation to pre-qualified tenderers in order that appropriate costs are identified prior to award of the main construction contract. **(C)** The handover strategy shall address any special requirements relating to the following (as appropriate): 1) phased handover of the project; 2) commissioning and acceptance testing; 3) handover information and guidance; 4) pre-handover training of personnel; 5) aftercare arrangements; and 6) other factors crucial to effective security management.

MAN 3.10 Control of Project Work at the Facility	
New Facility In-Use	**(A)** In cooperation and coordination with the facility Security Manager(s), the project Security Manager(s) shall establish, document, maintain and communicate any temporary security controls required for the duration of the project. *Note: In the case of projects involving construction works, this is often referred to as a Project or Construction Security Management Plan.* **(B)** Temporary arrangements shall address: 1) security risks to new assets associated with the project works (if any); 2) security risks to existing assets at the facility as a result of temporary project activities e.g. site clearance, construction, demolition; and 3) incident identification, management and recovery for the designated project site and any implications on the existing facility. **(C)** The facility Security Manager(s) will be responsible for implementing temporary measures related to existing assets (outside the designated construction site), while the project Security Manager(s) shall be responsible for the implementation of temporary measures related to the designated project site (unless otherwise specified by the project contract).
MAN 3.11 Project Commissioning & Security System Testing	
New Facility In-Use	**(A)** Commissioning and testing of all new or modified facility security components and systems shall be carried out to ensure that the performance of the facility security controls (physical and technological) is in accordance with the facility security design. **(B)** The main contractor shall be responsible for project commissioning unless otherwise specified by the project contract. **(C)** The project Security Commissioning records shall be incorporated within handover information to the Employer Representative(s).

MAN 3.12 Project Handover	
New Facility In-Use	**(A)** The project Security Manager(s) will manage the handover of the project unless specified otherwise in the project handover strategy and project contract. **(B)** The handover shall be implemented in accordance with the handover strategy. Successful project handover shall be signified by completion of: 1) tasks outlined in the handover strategy; 2) facility security commissioning; and 3) handover information. **(C)** Project close out shall not occur until sign-off is received from the Employer Representative(s).
MAN 3.13 Project Aftercare	
New Facility In-Use	**(A)** To ensure the facility security systems operate and where relevant adapt in accordance with the strategic intent and operational demands, for an agreed period following project handover, the project Security Manager(s) shall provide post-handover aftercare and support to the owner and/or Responsible Person(s) in accordance with the project handover strategy.

3.2.4 Security Innovation Section

The requirements in this section reward exemplary performance and the adoption of innovative facility security solutions which:

1) Address previously unresolved security need(s).
2) Are more effective or more efficient than existing solutions at meeting the security need(s).
3) Offer secondary benefits to end users and/or interested parties in addition to satisfying the security need(s).

INN 1: Innovation *Recognise and encourage innovation and an 'aspirational' approach to security risk management that improves facility security performance and provides learning opportunities for wider dissemination*	
CORE TECHNICAL STANDARD REQUIREMENTS	
INN 1.1 Facility Performance	
New Facility In Use	**(A)** The facility demonstrates exemplary security performance i.e. goes beyond best practice; in terms of any of the assessment areas covered in this standard.
INN 1.2 Innovation in Management	
New Facility In Use	**(A)** An innovative policy, process or procedure is used to improve the security performance of the facility. **(B)** Contribution to a collective security initiative(s) that benefits the facility, its neighbours and the wider community. *Note: An innovation may be evidenced at any stage in the built asset life cycle e.g. during design, an innovation that leads to better integration; or in-use, the deployment of innovative incident management procedures.*
INN 1.3 Innovative Facility Planning & Design (Physical Environment)	
New Facility In Use	**(A)** Innovative facility planning and design is used to improve facility security performance.

INN 1.4 Physical or Technological Innovation	
New Facility	**(A)** An innovative security technology e.g. software, component, sub-system or system is used to improve the security performance of the facility.
In Use	
INN 1.5 Innovation in Personnel Security	
New Facility	**(A)** Innovation in personnel security is used to improve facility security performance.
In Use	
INN 1.6 Data Application	
New Facility	**(A)** Data available at the facility is used pro-actively and in a timely manner to improve facility security performance. *Note: A wealth of data is now available from sensors within buildings and infrastructure e.g. building management systems, active surveillance systems or guard force reporting. This data is often discarded as a result of its value not being recognised and due to Data Protection requirements.* *The analysis and application of data, such as changes in user behaviours or incident performance may offer a range of security risk management benefits, particularly if data can be harvested in real-time and used for dynamic risk assessment and decision making.* *Care is required in utilising data to ensure compliance with privacy laws and data protection requirements.*
In Use	

4 CLASSIFICATION AND DESIGNATION

The SABRE Rating of a facility is determined by assessment against the Technical Requirements of this Standard. Increasing conformity with the Standard increases the scores achieved in the individual assessment sections and the overall SABRE Rating of the facility.

Weightings are applied to each Technical Requirement and each section of the Standard, and correspond to the relative importance of an issue on overall facility security. The weighting system is derived using a combination of consensus based weightings and ranking by a panel of experts. For the detailed breakdown of weightings for each assessment section, please refer to SD0229.

The SABRE Rating benchmarks are presented in Table 1. These benchmarks enable an applicant and interested parties to compare the facility under assessment with other SABRE rated facilities and a stock of facilities generally.

Table 1 SABRE Rating Benchmarks

SABRE Rating	% Score	Broadly representative of the levels of compliance at:
Outstanding	≥80	Less than top 1% of facilities
Excellent	≥70	Top 10% of facilities
Very Good	≥60	Top 25% of facilities
Good	≥50	Top 40% of facilities
Acceptable	≥40	Top 50% of facilities

A SABRE score of less than 40% and/or failing to meet SABRE minimum standards represents performance that is non-compliant with SABRE and these facilities are not eligible for a SABRE Rating or LPCB certification.

A SABRE Rating is valid at the time of certification. Internal and external factors, for example: changes in facility use, users and management; will potentially result in changes to the SABRE Rating. For this reason, the scheme requires on-going assessment if facilities are to remain part of the scheme. For scheme rules and information relating to ongoing certification, please refer to SD0229.

5 ADDITIONAL GUIDANCE DOCUMENTATION

Additional information regarding SABRE assessment and LPCB certification using the Technical Criteria outlined in this Standard, can be found in Scheme Document SD0229. Scheme Document SD0229 does not form part of this Standard and is not publicly available, but rather is available only to existing scheme members and new applicants to the scheme.

BRE Global Limited has produced the SABRE Essentials series of briefing papers to provide essential scheme information and outline scheme benefits for those considering joining the scheme. These can be downloaded at www.bre.co.uk/SABRE.

6 PUBLICATIONS REFERRED TO

SD0229	SABRE – Security Assessment and Certification for Buildings and Built Infrastructure Assets

7 AMENDMENTS ISSUED SINCE PUBLICATION

DOCUMENT NO.	AMENDMENT DETAILS	SIGNATURE	DATE