Infrastructure for New South Wales

Walsh Bay Arts Precinct

Security Design Brief

251710- SDB-04

Revision 4 SSDA | 14 November 2016

This report takes into account the particular instructions and requirements of our client.

It is not intended for and should not be relied upon by any third party and no responsibility is undertaken to any third party.

Job number 251710-00

Arup
Arup Pty Ltd ABN 18 000 966 165

Arup
Level 10 201 Kent Street
PO Box 76 Millers Point
Sydney 2000
Australia
www.arup.com

Contents

Page

1 Executive summary

1.1 Overview

Walsh Bay is a significant heritage precinct located on the arts and cultural ribbon; identified in the 2014 State Infrastructure Strategy.

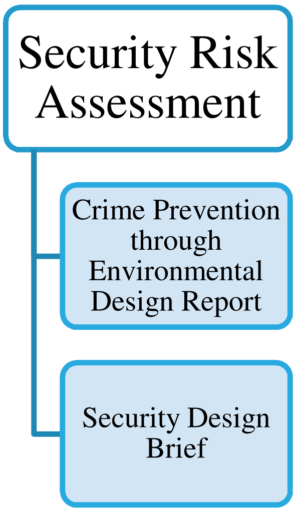
Walsh Bay Arts Precinct (WBAP) will create a sustainable and activated arts and culture precinct that supports and nurtures NSW's and Sydney's home-grown culture and creativity.

Arup has been engaged to provide security consulting services to the WBAP project; identifying opportunities for improvements and recommending security strategies to reduce the precincts exposure to security risks.

1.2 Security reports document list

This document forms part of a developing family of security reports that Arup are producing as part of our professional services to the Walsh Bay Arts Precinct Project. The Security Risk Assessment is the overarching security document supported by more detailed advice provided in the Crime Prevention through Environmental Design Report and this Security Design Brief.

The Security Risk Assessment provides a broad identification of the threat and risk profile facing the WBAP, and outlines possible treatments. These treatments are then detailed in the underlying reports.



1.3 Document purpose

This security design brief has been produced based on the outcome of the Security Risk Assessment and Crime Prevention through Environmental Design assessment. This security design brief aims to take the outcomes of those assessments and develop them into a comprehensive security strategy that if ratified, will form the Security Services designs during the ensuing project phases.

Appendix A contains a full list of recommended physical security, electronic security, security management, and crime prevention through environmental design measures to be considered for implementation. These recommendations aim to reduce the security risks identified within the Security Risk Management Report to as low as reasonably practicable, improve the WBAP design and layout from a crime prevention perspective, and help with the operation of the WBAP, both day-to-day and during events.

1.4 Protective security strategy

The recommended protective security strategy includes:

- Increasing the risk for would be offenders by improving security lighting, hardening perimeter entry/exit points to attack, and layering security based on the type and use of the space (public, semi-public, semi-private, and private);
- Securing loading docks and vehicular entry ways;
- Reducing opportunity for illegitimate vehicular access to the precinct; and
- Managing external events through the use of temporary fencing.

1.5 Electronic security strategy

The recommended electronic security strategy includes:

- Improving CCTV surveillance throughout the precinct to provide coverage of all vital areas for live monitoring and incident review/investigation;
- Providing electronic access control throughout the precinct to reduce opportunity for trespass, theft, and misuse of space;
- Providing intruder alarms to monitor commercial and sensitive areas outside of normal working hours;
- Managing physical keys through an electronic key management system;
- Providing a duress/help point system throughout the precinct for emergency communications by patrons and staff in case of a security incident;
- Providing an IP intercom system for the precinct; and

- Implementing an overarching security management system to provide a central point of control and interface with the precincts electronic security systems.

1.6 Security management strategy

The security management strategy for the precinct should:

- Provide security awareness training to staff;
- Develop a comprehensive set of security policies and procedures;
- Provide ticket security to prevent unauthorised access to events; and
- Provide loading dock security, and manage these securely.

2 Project overview

2.1 The Site and Surrounds

The Walsh Bay Arts Precinct (WBAP) (the "site") generally comprises Pier 2/3, Pier 4/5 and its shore sheds which make up Wharf 4/5, as well as the adjoining waterway. The site has a street frontage to Hickson Road. The site is shown in Figures 1 and 2. The site is part of the Walsh Bay area which is located adjacent to Sydney Harbour within the suburb of Dawes Point. The site is located within the City of Sydney Local Government Area.

Walsh Bay is strategically located to the north of Sydney's CBD in the vicinity of major tourist destinations including the Sydney Harbour Bridge, the historic areas of Millers Point and The Rocks, Circular Quay and the Sydney Opera House. The Barangaroo redevelopment precinct is located immediately to the south-west.

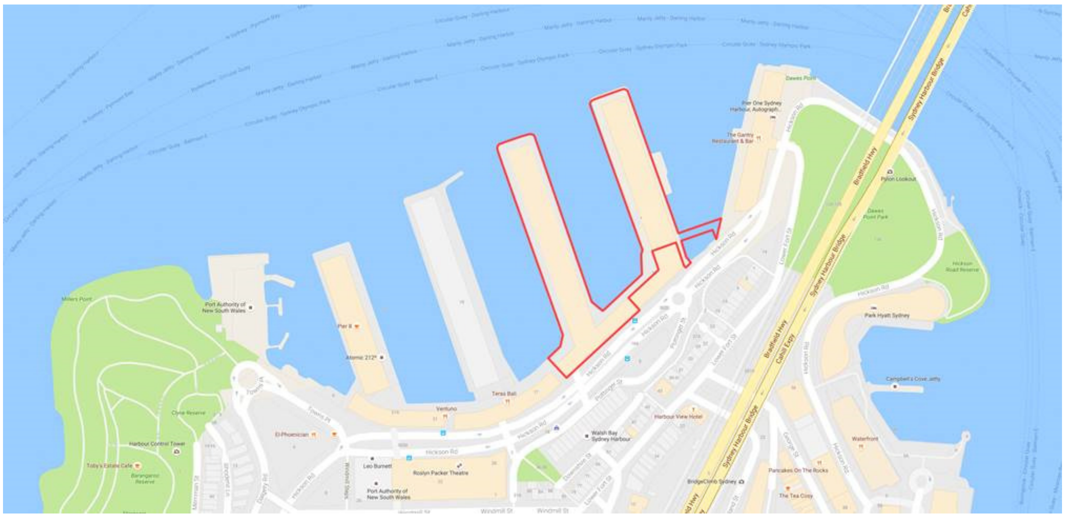


Figure 1. Site Location (Source: Google Maps)

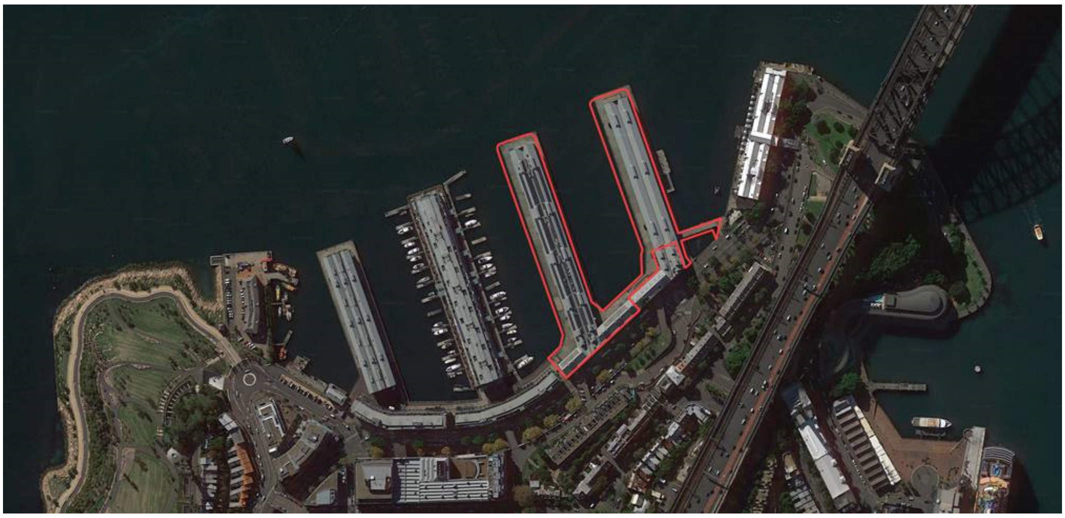


Figure 2. Aerial view (Source: www.nearmap.com)

Pier 2/3 is legally described as Lot 11 in DP 1138931 and Wharf 4/5 is legally described as Lot 65 in DP 1048377. The total area for these lots is 18,090sqm.

The land owner of the site is the Roads and Maritime Services (RMS). Both Pier 2/3 and Wharf 4/5 are occupied under various lease arrangements with Arts NSW, Department of Justice, primarily for arts and cultural uses.

The area of water that the project proposes to build over is also owned by RMS. Its land title description is Lot 12 in DP 1138931.

Walsh Bay comprises ten berths constructed between 1908 and 1922 for international and interstate shipping. These are collectively known as the Walsh Bay Wharves. The Walsh Bay Wharves Precinct is listed as an item on the State Heritage Register.

The Walsh Bay Wharves comprise the following:

- Pier One which contains the Sebel Pier One Sydney Hotel;
- Pier 2/3 the last remaining undeveloped pier (has previously received approval for cultural uses, temporary arts events and some commercial events);
- Wharf 4/5 which is occupied by the Sydney Theatre Company (STC), the Australian Theatre for Youth Program (ATYP), Sydney Dance Company (SDC), Bangarra Dance Theatre and the choirs comprising Gondwana, the Song Company and Sydney Philharmonia;
- Pier 6/7 which has been redeveloped for residential apartments and associated boat marina;
- Pier 8/9 which has been redeveloped for office uses; and,
- Shore sheds aligning Hickson Road which contain a range of commercial activities, including restaurants, bars, shops and offices.

2.2 The Project

The approved Stage 1 development application comprised:

- A new waterfront public square between Pier 2/3 and Wharf 4/5;
- A series of new lifts, stairs, and balconies on Pier 2/3 and Wharf 4/5 and modification to the roof of Pier 2/3;
- The inclusion of new tenancy spaces in Pier 2/3 and Wharf 4/5 for arts and cultural activities; and,
- The use of the precinct for arts festivals, events and pop-ups and associated uses, including restaurants, cafes and bars.

The WBAP Stage 2 State Significant Development Application seeks consent for construction works for the above to realise the WBAP project, as well as the proposed external alterations and additions to all of Wharf 4/5. It also seeks consent for new commercial and event uses in the precinct. Key aspects of the proposed development are outlined below:

Early works

- Early construction works comprising infrastructure upgrades, demolition, hazmat removal and sub structure works.

Pier 2/3

- Internal alterations and reconfiguration to provide for the following:
  - Performance venues;
  - Rehearsal rooms, production workshops, back of house facilities and offices;
  - Function spaces, bars, cafes and foyer spaces extending onto external gantry platforms (balconies) providing breakout space for internal foyers and allowing views of outdoor performances;
  - Mezzanine spaces for offices and back of house facilities;
  - Upgrades to meet compliance with current BCA, DDA and fire codes;
  - New lifts and stairs;
  - Creation of new commercial tenancies and public toilets;
  - Removal of some storey posts and beams to facilitate internal reconfiguration and new uses; and
  - Retention of a large proportion of the ground floor in its existing 'raw' heritage state for events and festivals including Sydney Writers' Festival and Biennale including venue and commercial hire.
- External alterations and additions comprising:
  - New balconies and external stairs for fire egress;
  - New external lift for access;
  - Installation of glazing in existing cargo sliding door openings and other solid panels on the eastern, western and northern elevations to allow for views into and out of the building;
  - Roof penetrations within the central valley at the southern and northern end to accommodate new performance spaces and associated structural modifications including truss strengthening;
  - Installation of ESD elements, such as photovoltaic panels and seawater heat exchange systems; and
  - Raising of the external floor level on the eastern side by introducing a new raised deck and continuous set of stairs beyond the existing column line.

Wharf 4/5

- Internal alterations and reconfiguration to the Bangarra Dance Theatre (BDT) tenancy to provide for the following:
  - Upgrade of the main rehearsal and performance spaces;
  - Upgraded foyer and exhibition space along the eastern frontage;
  - Improved office space at mezzanine level including a new lift and stairs;
  - Provision of a function space at ground level of the northern end of wharf with associated kitchen facilities; and
  - New entrance and new glazing in bays of sliding cargo doors, opening up the foyer and main studio to the Pier 4 apron.
- Minor internal alterations and additions to the SDC tenancy comprising:
  - Reducing the existing workshop space to create a fifth dance studio; and
  - Upgrading office and reception areas.
- External alterations and additions to SDC tenancy comprising:
  - Raising of the timber wharf deck adjoining the SDC café and opening of the facade with new glazing to activate the waterfront square.
- Creation of new commercial tenancies and public toilets;
- External fabric alterations around the Sydney Theatre Company (STC) tenancy comprising:
  - Improved street entry at Hickson Road involving relocation of the stairs to allow for an improved landing and point of arrival to the STC;
  - New ‘gantry’ balconies, stairs and lifts mid-wharf and at the end of the wharf to provide for improved accessibility and compliance with fire engineering solutions;
  - Minor amendments to the existing façade to accommodate new entries and exits along the wharf;
  - Roof penetrations within the central valley at two locations to accommodate theatre and workshop spaces and associated structural modifications including truss strengthening; and
  - Reinstallation of existing photovoltaic panels where applicable.

<u>Wharf 4/5 Shore Sheds</u>

- Internal alterations to reconfigure the choir spaces, including provision of a mezzanine for choir administration;
- Creation of new commercial tenancies at ground and mezzanine levels; and

- Provision of office space at ground level.

Public Domain

- Construction of a new waterfront square comprising a deck on piled structure:
- Shaded informal performance space on piled structure; and
- Changes to existing levels and steps down to facilitate access between the existing apron and new waterfront square.

New Uses

- Use of the precinct for arts festivals, events and pop ups as well as a range of activating uses such as retail, restaurants, cafes and bars.

3 Security principles

The security design brief for WBAP has been developed through several underlying security principles which are discussed below. These underlying principles provide a holistic approach to mitigating security risk for the precinct.

These security principles will be applied to the treatment measures outlined in the following sections of the Design Brief. These treatment measures have been identified as outcomes of the Security Risk Assessment.

3.1 Defence in depth

To effectively design a security system, security measures should be layered to provide a succession of concentric barriers around an asset (Figure 3). This design principle underlies all security advice provided to the WBAP. Ideally, each layer in a security strategy will require an adversary to conduct a separate and distinct act from the last, increasing the complexity of defeating the overall strategy. Such an approach increases uncertainty for would-be adversaries, increases their preparation and skill requirements, and increases the probability that any attempted act will be unsuccessful.

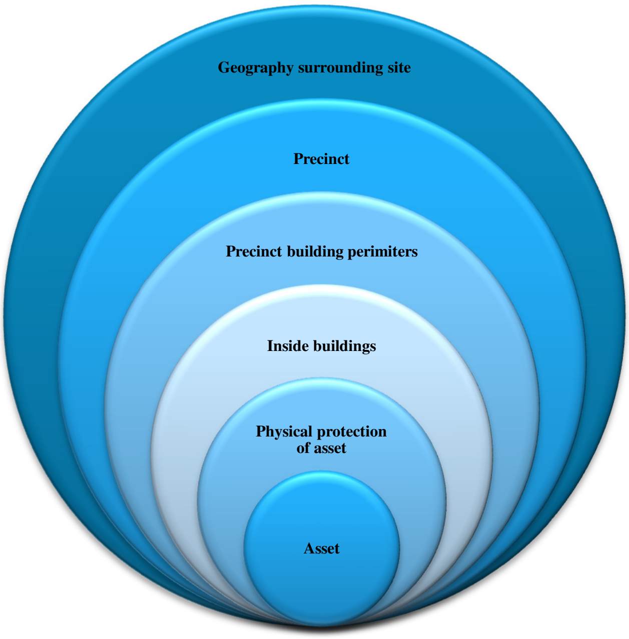

Geography surrounding site
Precinct
Precinct building perimiters
Inside buildings
Physical protection of asset
Asset

Figure 3. Defence in Depth

Effective defence in depth design will increase the time it takes for an adversary to reach an asset, while increasing the probability that they will be detected at the earliest possible point of misconduct. This detection will allow a suitable response to intervene before the adversary has achieved their goal; whether vandalism, theft, assault or other actions of security concern.

3.2 Deter, detect, delay, respond

Deter, detect, delay, and respond (D^{3}R) are the core components of a security protection strategy. They are embedded in the security advice provided to the WBAP. Ideally, each layer of protection within a defence in depth approach to security would have some form of deterrence, detection, delay, and response capability, however this is not always possible to achieve.

3.2.1 Deterrence

The purpose of the deterrence is to incorporate a variety of security measures that can be used to reduce the likelihood of opportunistic crime from occurring. Deterrence is achieved by increasing the perceived risk of detection or effort required to commit a crime.

Security methods such as signage, adequate lighting levels, CCTV coverage, and Crime Prevention through Environmental Design (CPTED) can deter opportunistic crime from occurring.

3.2.2 Detection

In order to minimise the loss or damage of assets, it is important to be able to detect unauthorised access into a protected area.

The security protection system should accurately detect an offender at the earliest possible point in order to provide the appropriate response the longest time possible to respond. The earlier the positive detection of an adversary, the less likely offenders will be able to reach the desired asset or achieve their goal before being apprehended.

The detection function of the D^{3}R security principle can be achieved by installing and using passive infrared (PIR) volumetric detectors in nominated rooms/locations, installing recessed magnetic reed switches, and installing and monitored CCTV. By ensuring the site has appropriate illumination and has clear sight lines and natural surveillance can also significantly improve the ability to provide the detection function.

3.2.3 Delay

When unauthorised access to a restricted space has occurred, it is important to delay the progress of the intruder to prevent and minimise the loss or damage of assets. This delay can be achieved through a series of barriers such as fences, locks, safes, doors, windows and walls. Ideally the length of delay should be greater than the time for a response force to arrive, in order to apprehend the offenders before they reach the asset or leave the facility after completing their objective.

Achieving effective delay in a publicly accessible space is difficult to effectively achieve.

3.2.4 Respond

A timely and appropriate response is required at the WBAP by in-house, contract security or the local Police, depending on the nature of the events.

3.3 Crime prevention through environmental design

CPTED is a contemporary design practice that aims to design out the opportunity for certain types of crime to occur in a particular location. A formal CPTED review and analysis has be undertaken for WBAP (CPTED Report).

CPTED is the process of designing the built environment to passively deter crime using a combination of three elements: natural access control, natural surveillance, and territoriality. CPTED does not rely solely on the implementation of physical barriers as part of an overarching Defence in Depth approach, but can also include psychological influences (soft solutions) such as lighting, music, ground coverings etc. The aim of the passive strategies is to improve crime deterrent characteristics of the precinct.

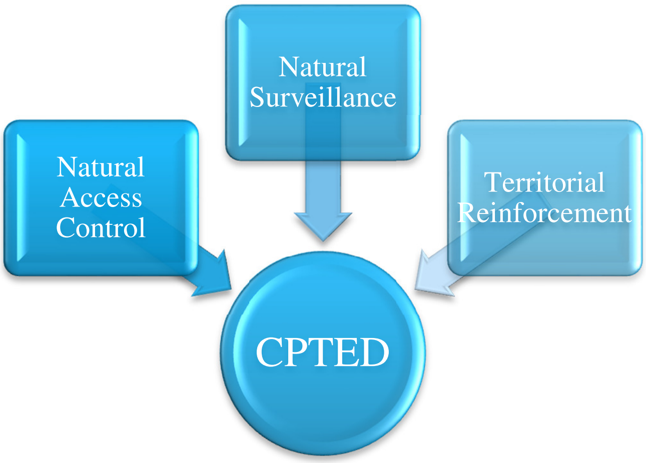


Figure 4. Crime Prevention through Environmental Design (CPTED)

3.3.1 Natural access control

Natural access control is the limitation of access to and through an area in order to create the perception of improved space ownership and purpose. It allows facility operators to influence how users gain access to an area and the conditions in which they do so.

Natural access control creates surety and improves way finding for legitimate users whilst reducing the ability for illegitimate people to access and egress the facility without being noticed, approached or apprehended.

3.3.2 Natural surveillance

Natural surveillance is the implementation of open space, improving site lines, and limiting the ability for illegitimate people to conceal themselves and their activities. Improved lighting to critical thoroughfares and mass gathering areas assists with the implementation of this concept. The use of glass partitions, walls and large windows increases the natural surveillance characteristics of an area, improves the propagation of light, and increases the range and coverage of CCTV cameras that may be operating in the vicinity.

3.3.3 Territoriality

Territoriality is the demonstration of space ownership and functional purpose to create a more harmonious and attractive place for legitimate users to gather while deterring illegitimate users from carrying out crimes and misdemeanour acts. This is most clearly advertised through the upkeep of the facility, ensuring that equipment and surfaces that are damaged through acts of vandalism or theft are quickly repaired and replaced. The cleanliness and neatness of the space is also an important factor that has a positive territoriality effect.

4 Security zoning

Security zoning is the process of delineating space within a precinct; identifying areas of public or restricted access, and providing appropriate security controls to restrict movement between these zones to legitimate users. In cultural and arts precincts, the naturally open and inviting space requires careful control to restrict the movement of the general public to nominated areas without imposing an aggressive security presence. To effectively achieve security control in such a way, careful consideration of the space, its natural barriers, and human behaviour is required.

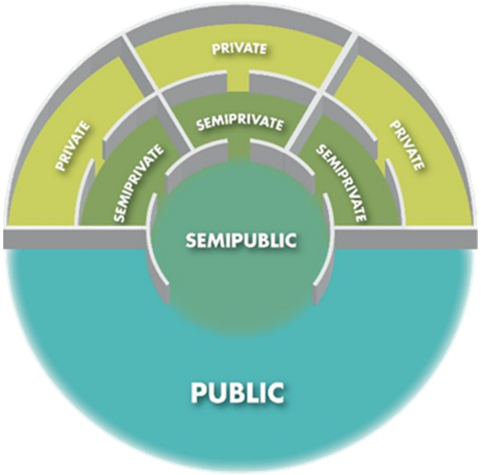


Figure 5. Security zoning

4.1 Public areas

Public space is considered any area that can freely accessed by the general public without any paid or special privilege. Public areas are considered uncontrolled from a security perspective, and must be carefully monitored by security personnel. Cultural precincts such as Walsh Bay have significant areas of publically accessible space. In context, these public spaces are vital for the activation of the precinct, and should be as welcoming and inviting as possible. These spaces include:

- Exterior spaces such as the waterfront square;
- Lobby's, receptions and foyers;
- Cafes, restaurants, bars;
- Public toilets; and
- Any other generally accessible areas without a performance ticket or special access privilege.

Public spaces should be protected in architecturally sensitive ways, drawing from CPTED principles in the first instance, and minimising the use of overt physical security controls. Surveillance of public spaces alongside efficient emergency or security response is vital for effective protection.

4.2 Semi-public areas

Semi-public space is considered any areas that is accessible by the public through special or paid privilege. Semi-public areas are still largely uncontrolled from a security perspective, however these areas are generally restricted to paying members of the public, staff, performance members, and VIPs. This restriction is achieved by clearly delineating the space and performing cursory security checks to ensure individuals have a valid ticket or purpose to be in the area.

For WBAP, semi-public areas would be considered:

- Shared foyers;
- Auditoriums;
- Performance spaces;
- Theatres; and
- Any other ticketing restricted areas.

Semi-public space should be protected by slightly more overt security measures such as physical barriers (doors, locks, ticket counters, ticket gates), electronic security measures (CCTV, access control, intruder alarms for after hours), and staff (ticketing officers).

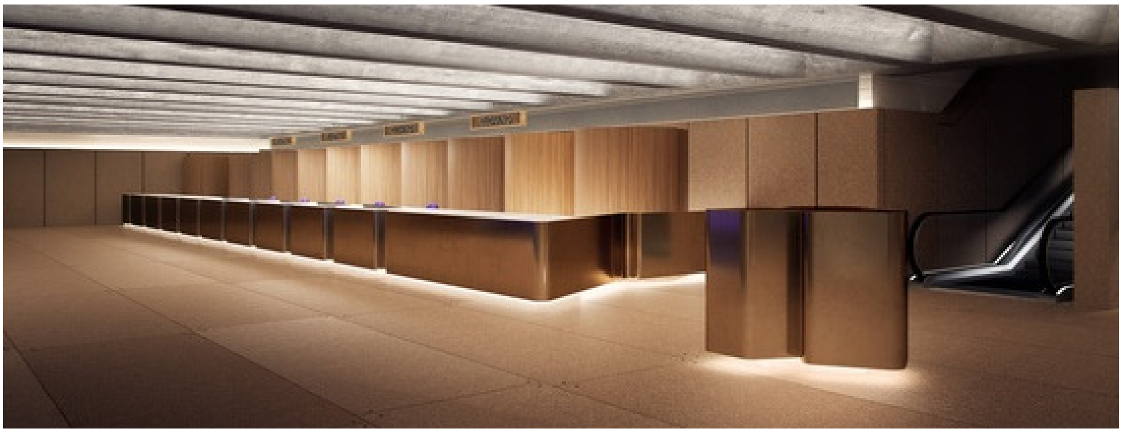


Figure 6. Example ticketing area

It is important that these spaces are open, inviting and focussed on the customer experience, but restricted through clear security boundaries that are reinforced by staff and the architectural design of the space.

4.3 Semi-private areas

Semi-private spaces are considered areas restricted to precinct staff, performance staff and crew, technical crew, restaurant, café, and bar staff, and other similar people. Semi-private space must be clearly segregated from semi-public and public space, and restricted to authorised users only. Semi-private space is considered controlled from a security perspective, and would generally require an electronic access control credential or mechanical key to gain entry.

Such areas at WBAP include:

- Loading docks;
- Performance preparation spaces;
- Rehearsal spaces;
- Performance crew areas;
- Staff breakout spaces;
- Technical production areas (audio, lighting, etc.);
- Laundry, board rooms, wardrobe, freezers, cool stores, costume stores, workshops etc.;
- Restaurant/bar back of house areas;
- Commercial and tenanted areas;
- Precinct management offices; and
- Any other performance back of house areas.

Entry into these back of house areas should be monitored and controlled. CCTV surveillance is not required in all areas, but may be required at entry/egress points. Back of house areas should be functional and easily navigable, however security controls will place some restriction of free movement to increase the difficulty of illegitimate users accessing the space.

4.4 Private areas

Private areas are considered areas that are only accessible to precinct staff members or that are storing high value goods. Such areas should be controlled and monitored by CCTV, electronic access control and intruder alarm systems, alongside physical hardening of structure and doors as required.

Such areas include:

- Security monitoring centre;
- Communications and server rooms;
- Plant rooms;
- High value goods, artwork, equipment or physical assets storage; and
- Any other commercial or plant back of house areas.

Private space should be protected on a *'need to go'* basis, and staff should have a clear reason for accessing these spaces. At no time should the general public have access to these areas.

4.5 Variable Spaces

Due to the nature of event operations at WBAP, predefined areas will be subject to change with event conditions. These conditions will require flexibility with security operations strategies to provide effective protection from the identified security risks. The security management of variable spaces should be considered from a policy and procedures perspective, with aid from existing electronic and physical security systems.

5 Protective security strategy

The protective security strategy aims to increase the risk to potential offenders by improving passive security such as natural surveillance (making people more observable), while hardening selected areas to attack. This combination of physical security controls will deter opportunistic offenders, and increase the difficulty for individuals who have targeted the precinct for specific crimes (such as theft).

5.1 Signage

Security signage is an important component of a passive security strategy, as it provides a deterrent to opportunistic criminals. Signage should be prominently displayed throughout the precinct, particularly along heavily trafficable areas and main entrances. Signage should outline the use of CCTV, identify help point locations, and provide emergency service and security telephone numbers.

Signage should include:

- Security and emergency telephone phone numbers;
- *CCTV in operation*;
- Security officers patrol this area; and
- *Emergency help point*, and instructions for use where relevant.

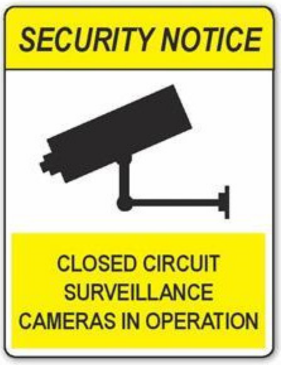


Figure 7. Example CCTV in operation sign

Signage should not be placed or mounted in such a way as to provide a climbing aid.

5.2 Security lighting

Security lighting acts as a deterrent to opportunistic crime as it increases the visibility of potential offenders to passer-by. Security lighting also aids electronic surveillance systems capture higher quality imagery. Lighting should at minimum comply with Australian standard AS1158 P category 7 (public activity areas).

Nominated pathways along piers and throughout the precinct should at minimum comply with the Australian Standard AS1158, P category 2 (public pathways and cycle-ways). This lighting will provide deterrence against anti-social behaviours, crimes conducted at night, and increase the perception of safety for individuals along designated routes.

The lighting design provided should meet Australian standard AS1158 as a minimum, and provide a consistent and uniform level of illumination that reduces dark spots and shadowing as much as practical.

5.3 Vandalism and graffiti

Vandal resistance should be considered as a design factor in the chosen construction material and methodology, particularly for outdoor, public furniture and fixings. Construction should be of a robust standard; joints, screws and other fixings should be hardened and concealed where possible.

Public tables and seating should be designed to resist scratching and shattering, and porous construction materials should be fully sealed and easily cleanable to remove graffiti.

5.4 Mechanical locking systems

Mechanical locking systems used for storage areas, equipment rooms, or other back of house areas should be of a high security type. Locking systems should be SCEC endorsed with restricted key profiles to provide pick, bump and drill resistance.

Locksets installed in doors should be protected with strike shields on the unsecure side of all outward opening doors, to limit the possibility of a forced door attack.

5.5 Doors

External doors should be of robust solid core construction, steel or timber. Where external doors are sliding or glazed, vandal resistance materials (scratch, shatter) should be provided. This should be achieved by an anti-shatter film, and the door frame should be reinforced.

Internal doors leading to semi-public or semi-private areas that are not ticket or guest entry points should be access controlled to restrict access to legitimate users (i.e. staff).

Internal doors leading into private (secure) areas should be solid core doors. Such doors should be access controlled (read-in). Door locking mechanisms should be electric strike or electric mortise lock.

All external, semi-private and private doors should be monitored by the intruder alarm system and electronic access control system through a flush mounted reed switch.

5.6 Windows

To provide holistic perimeter protection, external glazing should be protected to a similar level as entranceways throughout the precinct. It is recommended that external windows throughout the WBAP should be tempered and/or laminated with a Polyvinyl Butyral (PVB) interlayer to improve intruder resistance.

5.7 Pits

Communication and service pits should be appropriately secured, with access points protected by SCEC endorsed security pit locks. Pits should be vandal and intruder resistant, constructed of concrete or a high strength composite variant.

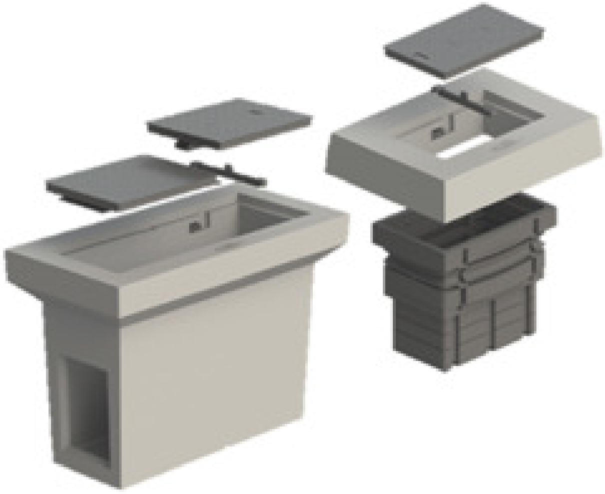


Figure 8. Example pits

5.8 Roller shutters

There are several vehicular entries into the WBAP, including through loading dock type areas facing onto Hickson Road. To prevent unauthorised access through these entry portals, barriers should be provided, enforcing a security checkpoint before vehicular entry is granted to the site.

Such measures should include manually removable bollards along the frontage of the designated vehicle entry points. Further, the inclusion of boom gates controlled by the electronic access control system should be provided for vehicle control during the day.

Roller shutters are proposed to provide a barrier between the publicly accessible roadway and the loading docks and broader WBAP. Shutters should:

- Be constructed from interlocking galvanised steel slats;
- Be automated and motorised; and
- Be powder coated a colour to suit architectural designs.

An anti-lift device should be installed on roller shutters as an additional security protection measure. Anti-lift devices provide protection against individuals attempting to manually lift the shutter when in a closed state. Without an anti-lift device, shutters are susceptible to individuals forcing the shutter open by hand or with tools.

Security shutters should interface with the precinct's electronic access control system. Interfacing with the EACS will provide security operations staff with the ability to control and manage the loading docks and precinct security system from a central location or locations, while receiving feedback as to the status of the system.

5.8.1 Safety considerations

There are several occupational health and safety considerations for the installation of security shutters. This includes the use of appropriate signage to identify potential crush or pinch points, and warnings about tailgating and other mistreatments.

It is recommended that photoelectric beams are installed with each shutter, which, when broken by an object will keep the shutter open; or stop the door from closing. It is recommended that photoelectric beams be provided with a covering shroud to reduce environmental factors affecting the PE beam's operation.

5.9 Temporary fencing

WBAP will host outdoor events in the waterfront square, which is normally publically accessible space between both piers. While this location is generally open to the public, restrictions on this access will have to be put in place during these external events if they are ticketed. Importantly, this restriction will have to be achieved in such a way as to reduce all possible entry points to the venue (i.e. through surrounding buildings) down to nominated and controlled entry areas to ensure a secure perimeter and ticket checking process is in place.

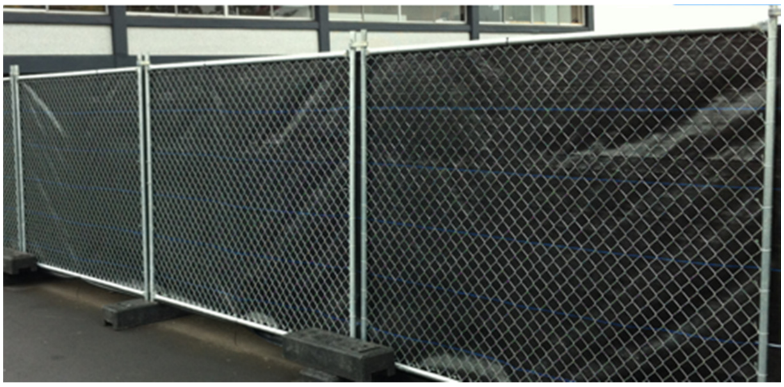


Figure 9. Example temporary fence

Temporary fencing can be arranged in such a way to restrict access to alternate entry paths and 'funnel' visitors to the ticketing areas. Temporary fencing should be of security height (minimum 2.4m high), with cladding or sheet covers to increase the difficulty of scaling, and limit visual transparency to reduce the opportunity for individuals to observe events without paying for entry.

5.10 Hostile vehicle mitigation

Hostile vehicle mitigation is a protective security strategy which can be implemented to prevent high impact events such as vehicle ram raids, the delivery of vehicle borne improvised explosive devices, and other such scenarios, involving motor vehicles.

The layout and building arrangement at WBAP does not provide significant opportunity for hostile vehicle style attacks to occur, however consideration should be given to car parking arrangements (below) and vehicular access to loading docks (Section 7.6).

5.10.1 Car parking

Car parking near offices or commercial areas on the WBAP piers should be prevented. Parking should be restricted to Hickson Road for all individuals working or visiting WBAP.

This parking arrangement ensures a secure perimeter is maintained around the precinct, and that potential hostile vehicles cannot enter the secure area under the guise of a legitimate purpose.

5.11 Communications rooms and server rooms

Communications and server rooms throughout the WBAP should be protected from unauthorised access. Due to the critical nature of such areas, clear audit access trails should be recorded for post incident investigation. Server rooms may house a variety of equipment, including security servers, audio/visual equipment and IT infrastructure.

It is recommended that communication and server rooms be protected by:

- Electronic access control (read in);
- SCEC endorsed mechanical locking system;
- Strike shields on outward opening doors;
- Solid core door (40mm minimum);
- Three hinge arrangement; and
- Electric strike or mortise lock.
- Physically robust doors, walls, ceiling and floor.

6 Electronic security strategy

The electronic security strategy has been developed to increase the difficulty for potential offenders, while providing a sophisticated personnel management system for the precinct. Electronic security systems provide substantial information for post-incident investigation and review, as well as provide real-time information for security operators to monitor and respond to as required.

6.1 Security management system

An integrated security management system (SMS) is recommended for the WBAP. The SMS should govern the electronic access control, intruder and duress alarm, intercom, and CCTV systems throughout the precinct.

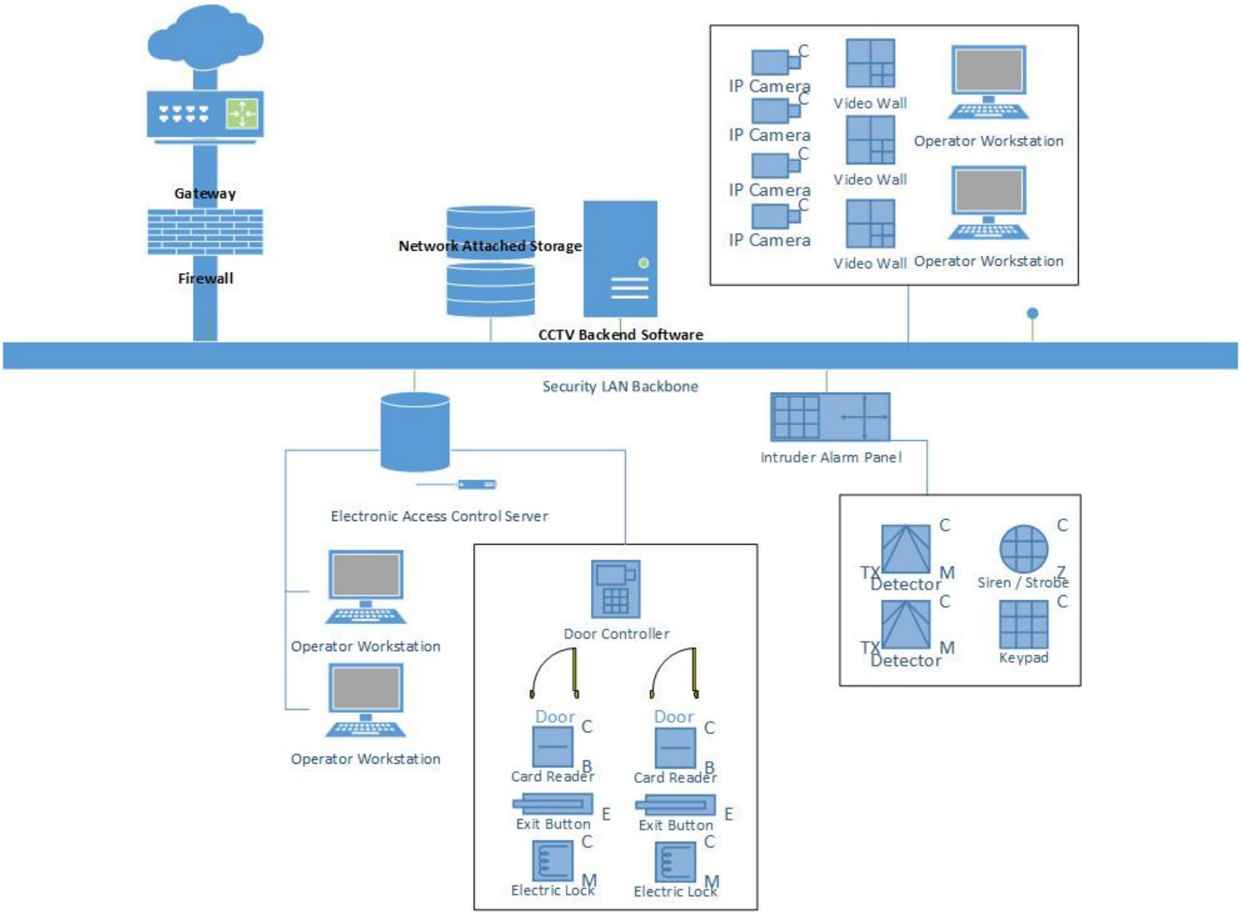


Figure 10. Example security management system

SMSs reduce uncertainty and complexity for security officers during electronic security system operation. Security operators interact with the system through one graphical user interface, actioning intrusion detection, CCTV, and electronic access control from one location. This arrangement makes training and operation for staff simple and straightforward, and provides more efficient operation in day to day and emergency activities.

6.1.1 Security network

A dedicated security network is recommended for the WBAP. A dedicated security network is physically and logically segregated IT network for the interconnection of security devices and equipment.

The security network should as a minimum:

- Be segregated from the existing IT network through a secure gateway;
- Operate within a VLAN;
- Be firewalled from the internet;
- Provide device access control measures through IEEE 802.1X or MAC address verification.

All security devices, including operator workstations, CCTV cameras, security servers, and access control equipment should communicate through this dedicated security network. Security devices connected to the network should have their default username and password login details changed upon installation.

6.2 Closed circuit television

An IP based network video surveillance system is recommended to provide coverage throughout the WBAP. This system should consist of high definition IP CCTV cameras, network switches, image storage devices, and other associated equipment as a minimum. This equipment should be connected to the security network.

The CCTV system should be monitored, controlled and administered from the security control room and operator workstations.

The provided CCTV System should perform a combination of the following core functions, as required:

- General display of video for ad-hoc security monitoring;
- Control room display for dedicated CCTV operations;
- Simultaneous playback of one or more IP camera video streams;
- Recording of the IP camera video streams, locally (on-site).

CCTV is a useful tool for post-incident investigation and review. CCTV does not stop the incidence of crime, but does provide security operators with increased situational awareness, and an improved capacity to respond to security incidents appropriately when they occur.

6.2.1 Cameras and camera coverage

It is recommended that existing CCTV cameras be replaced as required with digital megapixel CCTV cameras providing a minimum of 1080p resolution. This camera upgrade should include both replacement of existing cameras, and the installation of new cameras throughout the precinct to provide coverage of critical areas.

CCTV cameras should be of low profile dome type to reduce visual impact on the precincts architecture.

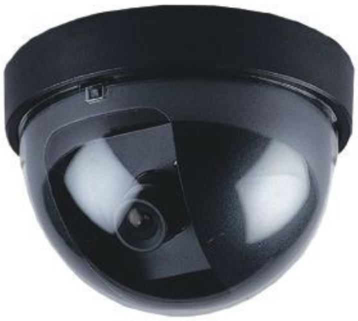


Figure 11. Example internal dome camera

External cameras should be vandal and weather resistant (IK09 and IP66 rating), and mounted at a height that reduces the opportunity for human interference. External camera fixings and screws should be of marine grade stainless steel, and camera housing should be designed to operate in a marine environment.

CCTV cameras should cover the following areas:

- Building entry/exit points;
- Precinct entry/exit points;
- Water based entry/exit points to the precinct;
- Cafes, restaurants, and bars;
- Cash handling areas;
- Lifts;
- High value item store entries/exits;
- Box office and ticketing areas; and
- Future temporary entry/exit points during events held in waterfront Square.

6.2.2 Recording and storage

CCTV footage should be kept to an evidentiary standard, with inbuilt watermark, time and date stamp, as well as clear identification of which camera footage was recorded from. This footage should be able to be exported and provided to investigators as required.

CCTV image recordings should be stored for 28 days as a minimum.

CCTV imagery should be stored in a central location within the precinct. This location should be a secured communications or server room.

6.3 Electronic access control

A centralised electronic access control system (EACS) is recommended for the WBAP. A centrally monitored and controlled system allows for easier maintenance of cardholder records and access rights, alongside operator certainty of ongoing events within the precinct. A centralised system increases operating flexibility and the capacity for security operators to make changes as needed to changing precinct circumstances.

It is recommended that the following elements and functionality are provided for the EACS:

- Configurable access zones and sub-zones;
- Anti-pass back controls;
- Collective controls (groupings of users, zones, access rights etc);
- Configurable access groups comprising users and their access rights to access zones, sub-access zones and individual portals, as well as date / time control;
- Configurable user information;
- Independent intelligent door controllers;
- Manual portal control;
- Interfaces with the CCTV system, fire system, lift system, and other motorised portals;
- Multi technology access cards and compatible readers; and
- Electric locking and control devices.

6.3.1 System architecture

The electronic access control system should be configured with several multi-door controllers, each communicating back to a central access control server (Figure 12). This architecture allows for simpler maintenance of the system, and less component parts to securely store.

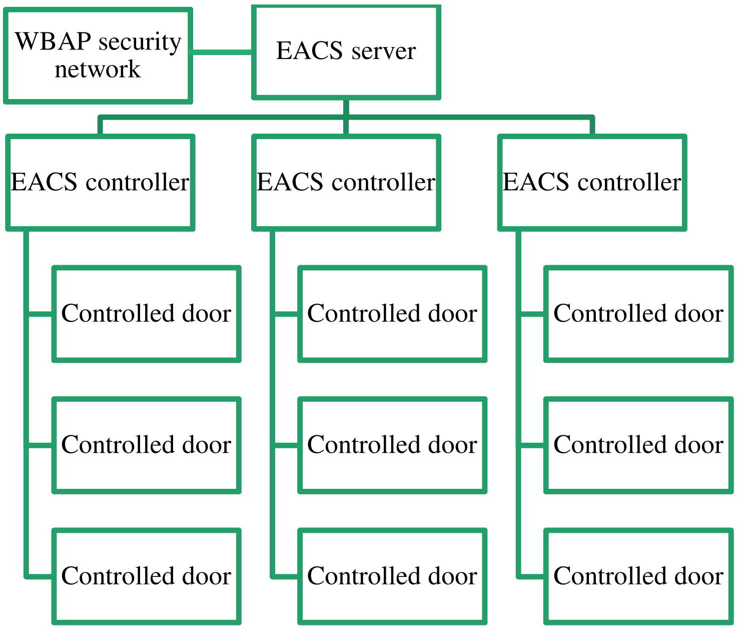


Figure 12. Example EACS system architecture

6.3.2 Access credentials and card readers

Card readers will be provided on access controlled doors to facilitate the electronically controlled access functionality. These readers should be multi-technology (125kHz, 13.56MHz, NFC, and Bluetooth) readers.

Authorised precinct staff and tenants should be provided with their own access card, programed to provide them with access to nominated access controlled portals. Staff will not automatically be provided with access to all access controlled portals at WBAP, but only those that they reasonably require access to, in order for them to carry out their assigned tasks.

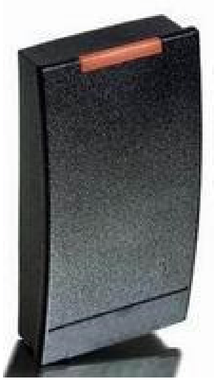


Figure 13. Example card reader

Card readers should be mounted adjacent to the associated portal, on the continuous accessible path of travel, and in clear line of sight of people approaching the portal.

The access cards provided at WBAP should be 13.56MHz contactless smart cards.

6.3.3 Electric locks

Electric locks should be provided on access controlled doors to facilitate the electronically controlled access functionality.

Electric locks throughout WBAP should typically be provided in the following situations:

1. Electric Mortise Locks; for timber single leaf doors, or double doors with the inactive leaf not electrically controlled. Door leaves must be hinged on the edge (not centrally pivoting, enabling the lock cable to pass cleanly from the frame to the leaf).
2. Electric Strikes; for fire stair doors, or existing doors where cable access for an electric mortise lock would be otherwise prohibitive. Examples include frameless glass doors, aluminium framed doors or centrally pivoting doors.
3. Electromagnetic Locks; for double doors where both leaves need to be electrically controlled.
4. Electric drop bolts; It is preferred that these are not used; due to door alignment reliability issues.

All electric locking solutions provided for WBAP should be fail-safe in operation, meaning the associated portal will unlock on loss of power to the lock.

6.3.4 Other equipment

Request to exit buttons and emergency break glass buttons should be provided to facilitate general or emergency egress through electronic access controlled portals.

Request to exit and emergency break glass buttons should be mounted adjacent to the associated portal, on the continuous accessible path of travel and in clear line of sight of people approaching the portal.

Request to exit and emergency break glass buttons should comply with and be mounted in accordance with AS 1428.1-2009 – Design for Access and Mobility.

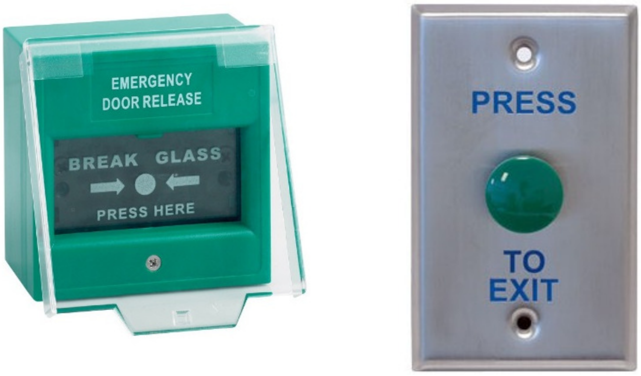


Figure 14. Example break glass button and REX button

6.4 Intruder alarms

Intruder alarm devices should be provided to monitor the integrity of nominated areas. Such areas will include:

- Valuable item/equipment stores;
- Cash handling areas;
- Back of house areas outside of operating hours; and
- Commercial and office spaces outside of operating hours.

Intruder alarm devices should use the same security control panels as the electronic access control system.

The system should comply with AS 2201 – Intruder Alarm Systems.

Monitoring, control and administration of the Intruder Alarm and Duress devices should occur at the security monitoring centre.

6.5 Duress and help points

Duress alarms should be provided in nominated high risk locations such as cash handling areas, and in accessible toilets.

Duress alarm system devices should consist of double push button style duress buttons (non-accessible toilets) that are either wall or under counter mounted (Figure 15). Accessible toilets should be of single push, wall mount design. Upon the activation of a duress device, a priority alarm will indicate the location of the alarm via a graphical display at the security monitoring centre.

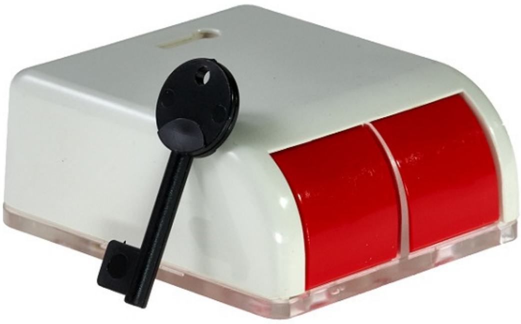


Figure 15. Example double push duress button (under desk variant)

Duress alarms should be latching such that the alarm does not automatically reset until acknowledged and processed at the security control room.

The fixed duress alarm system should interface to the IP CCTV system to provide recording and automatic display of camera views of the area in which a duress alarm is initiated.

6.5.1 Help points

An emergency help point system should be provided throughout the Precinct, particularly through waterfront Square. Such a system will increase the perception of safety, provide a deterrent against opportunistic crime, and provide users of the space the ability to contact security quickly when an incident occurs.

Help points should be installed in accordance with AS1428.

Help points should be IK09 and IP66 rated for impact and weather resistance.

The emergency help point system should operate using digital technology over an IP network, providing the following interactions when the help point button is pushed:

- Provide clear, undistorted voice communications, free from background noise and external distortion regardless of environmental surroundings; and
- Ability to automatically display the video from CCTV camera/s viewing the help point at the security control room.

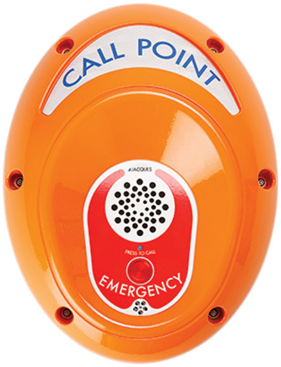


Figure 16. Example emergency help point

The emergency help point system should have a high level interface with the access control system and the CCTV system.

6.6 Electronic key control

A suitable electronic key management system should be provided that ensures a single orientation, positive key capture, with electronic access control to the cabinet. Electronic key control reduces the complexity of key management for precinct facility managers, improves the audit trail surrounding access to physical keys, and reduces opportunity for key theft and unknown misplacement.

Further considerations for an electronic key system include:

- Tamper resistance;
- Solid and intruder resistant construction;
- Integration with SMS / EACS;

- Option for multiple authentication to sign out high security keys (e.g. two person sign out);
- Key alarms;
- Maximum key issue per user; and
- Electronic Audit Trail.

Figure 17. Example electronic key management system

6.7 Intercom system

An IP Intercom System should be provided at nominated locations to aid visitor and staff interaction between remote doors. Intercom systems provide surety in visitor recognition, and reduce the opportunity for trespass by ensuring perimeter doors remain locked at all times. Existing intercom systems at WBAP should be upgraded to interface with the security management system, CCTV system, and electronic access control system.

Provided intercoms should be installed and mounted in accordance with AS 1428 – Design for Access and Mobility.

The IP intercom system should operate using digital technology over an IP network, providing the following interactions when the Door Station Intercom push button is pressed:

- Provide clear, undistorted voice communication, free from background noise and external distortion regardless of environmental surrounding;
- Ability to automatically display the video from CCTV camera/s viewing at the Door Station Intercom on nominated Operator Workstations; and
- Ability to automatically display or highlight the portal associated with the Door Station Intercom when used so the operator can remotely unlock the portal by clicking a master intercom button.

The intercom system should have a high level interface with the access control system and the CCTV system.

7 Security management strategy

The security management strategy provides an overview of security considerations in managing the daily operations of the precinct from a security perspective.

7.1 Central security monitoring centre

A central security monitoring centre (SMC) will be established to manage security for the WBAP and other Arts facilities managed by Arts NSW. The SMC will be coordinated by the Precinct Manager who will be responsible for the smooth, safe and secure operation of the precinct. This may be located at the precinct or outsourced to a third party provider, a decisions which is yet to be determined.

7.2 Security officers

Security officers provide physical security presence throughout the precinct, and are an important part of providing a deterrence effect to opportunistic crime. Security officers should irregularly patrol the precinct, especially at night, and check doors are closed and locked, and windows are secured after hours.

Contract security officers are recommended to be stationed at WBAP at all times, with increased staffing for events. It is recommended that two security officers are stationed on site, with one providing a roaming guard service and the other monitoring security feeds on the CCTV system, electronic access control system, and other dedicated security systems.

Security officers should be responsible for responding to alarms, duress, and emergency calls, investigating as required to determine the cause of such events.

During events, this staffing level should be increased as required, with extra costs associated being passed on to the event.

Security officers should be uniformed to be clearly identifiable and visible in the precinct.

7.3 Security awareness and training

Security awareness training is staff training that occurs on a regular basis through numerous avenues. For example, security awareness training could consist of an email campaign, security message posters, or formal presentations. Security awareness training is important to educate staff on their responsibilities and what to do when faced with a potential security incident. Further, security awareness training helps to build a security culture, which significantly reduces the possibility of insider risks.

7.4 Security procedures

The security management strategy should include comprehensive policy and procedures. Such procedures should include (but not be limited to):

- Suspicious package;
- Bomb threat;
- Terrorist attack;
- Active shooter;
- Help point and duress response;
- Unusual activity reporting;
- Clear desk policy;
- Computer and email usage;
- Information classification;
- Internet usage;
- Password protection;
- Social media usage;
- Media policy;
- Workplace violence;
- Alcohol management and abuse;
- Employee screening;
- Cash handling;
- Radio communications;
- Theft & loss prevention;
- Security investigations;
- Deliveries / delivery management;
- Key management, including lost key and re-keying;
- Access control management, including lost card;
- Precinct emergency shutdown and evacuation;
- Security coordination with emergency services;
- Business continuity;
- Forged or fraudulent tickets, ID, or other identifying documentation;
- Trespass, graffiti, vandalism or other criminal action;
- Post incident evidence handling;

- Event and external event operations;
- VIP or special event functions, including secure escort of individuals; and
- Protests or demonstrations.

The above is not meant to be an exhaustive list, but provides some indication of required security and staff procedures.

7.5 Ticketing

Ticket security is vital for effective and secure event management. As tickets are the only security identification check carried out by a venue before allowing a member of the public into a controlled area, care must be taken to ensure the ticket holder is legitimate.

Tickets have always been a target for duplication and forgery, and it is important to take measures to increase the difficulty and technical skill to carry out such activities successfully. Increasing ticket security improves revenue protection.

Some security measures that could be included in ticket printing include:

- Tamper evident holograms;
- Gloss marks;
- UV ink;
- Unique barcodes;
- Security micro text;
- Heat sensitive ticket paper; and
- Electronic tickets.

7.6 Loading docks

Loading docks are areas of security concern due to their interface with uncontrolled third parties such as delivery workers, and the secure access to back of house areas. This interface introduces a potential vulnerability to the overall security perimeter, and must be managed carefully.

Loading docks should be controlled areas of the precinct, with deliveries and arrivals monitored at all times. Vehicles approaching a loading dock should request access from a control point external to the dock, and should show some form of identification before entry is granted. The Precinct Manager can assist with efficient provision of this function.

Vehicles arriving should, where possible, be scheduled and expected the Precinct Manager.

This should be considered in conjunction with the Logistic Scheduling and Management strategy for WBAP.

Appendix A – List of Recommendations

ID	Type	Recommendation	Comment
Physical Security			
PS01	Signage	Should include: Security and emergency telephone phone numbers;	
PS02	Signage	*CCTV in operation*;	
PS03	Signage	Security officers patrol this area; and	
PS04	Signage	*Emergency help point*, and instructions for use where relevant.	
PS05	Signage	Signage should not be placed or mounted in such a way as to provide a climbing aid.	
PS06	Lighting	Lighting should at minimum comply with Australian standard AS1158 P category 7 (public activity areas).	
PS07	Lighting	Nominated pathways along piers and throughout the precinct should at minimum comply with the Australian Standard AS1158, P category 2 (public pathways and cycle-ways).	

ID	Type	Recommendation	Comment
PS08	Lighting	The lighting design provided should meet Australian standard AS1158 as a minimum	
PS09	Lighting	Provide a consistent and uniform level of illumination that reduces dark spots and shadowing as much as practical.	
PS10	Vandalism / Graffiti	Outdoor furniture should be of a robust standard; joints, screws and other fixings should be hardened and concealed where possible.	
PS11	Vandalism / Graffiti	Porous construction materials should be fully sealed and easily cleanable to remove graffiti.	
PS12	Vandalism / Graffiti	Public tables and seating should be designed to resist scratching and shattering	
PS13	Mechanical Locks	Mechanical locking systems used for storage areas, equipment rooms, or other back of house areas should be of a high security type	
PS14	Mechanical Locks	Locking systems should be SCEC endorsed with restricted key profiles to provide pick, bump and drill resistance.	
PS15	Mechanical Locks	Locksets installed in doors should be protected with strike shields on the unsecure side of all outward opening doors	

ID	Type	Recommendation	Comment
PS16	Doors	External doors should be of robust solid core construction, steel or timber	
PS17	Doors	Internal doors leading to semi-public or semi-private areas that are not ticket or guest entry points should be access controlled	
PS18	Doors	Internal doors leading into private (secure) areas should be solid core doors. Such doors should be access controlled (read-in).	
PS19	Doors	All external, semi-private and private doors should be monitored by the intruder alarm system and electronic access control system	
PS20	Doors	Door locking mechanisms should be electric strike or electric mortise lock.	
PS21	Windows	It is recommended that external windows throughout the WBAP should be tempered and/or laminated with a Polyvinyl Butyral (PVB) interlayer to improve intruder resistance	
PS22	Pits	Communication and service pits should be appropriately secured,	
PS23	Pits	Access points protected by SCEC endorsed security pit locks.	

ID	Type	Recommendation	Comment
PS24	Pits	Pits should be vandal and intruder resistant, constructed of concrete or a high strength composite variant.	
PS25	Roller shutters	Be constructed from interlocking galvanised steel slats;	
PS26	Roller shutters	Be automated and motorised; and	
PS27	Roller shutters	Be powder coated a colour to suit architectural designs.	
PS28	Roller shutters	An anti-lift device should be installed on roller shutters	
PS29	Roller shutters	Security shutters should interface with the precinct’s electronic access control system.	
PS30	Roller shutters	Appropriate signage to identify potential crush or pinch points, and warnings about tailgating and other mistreatments.	
PS31	Roller shutters	It is recommended that photoelectric beams are installed with each shutter	
PS32	Roller shutters	It is recommended that photoelectric beams be provided with a covering shroud to reduce environmental factors affecting the PE beam’s operation.	

ID	Type	Recommendation	Comment
PS33	Roller shutters	Such measures should include manually removable bollards along the frontage of the designated vehicle entry points	
PS34	Roller shutters	Further, the inclusion of boom gates controlled by the electronic access control system should be provided for vehicle control during the day.	
PS35	Hostile Vehicle Mitigation	Car parking near offices or commercial areas on the WBAP piers should be prevented.	
PS36	Hostile Vehicle Mitigation	Parking should be restricted to Hickson Road for all individuals working or visiting WBAP.	
PS37	Temporary fencing	Should be provided to restrict access during events in the waterfront square.	
PS38	Temporary fencing	Temporary fencing should be of security height (minimum 2.4m high), with, and	
PS39	Temporary fencing	cladding or sheet covers to increase the difficulty of scaling	
PS40	Temporary fencing	Limit visual transparency to reduce the opportunity for individuals to observe events without paying for entry.	

ID	Type	Recommendation	Comment
PS41	Communication rooms	Electronic access control (read in);	
PS42	Communication rooms	SCEC endorsed mechanical locking system;	
PS43	Communication rooms	Strike shields on outward opening doors;	
PS44	Communication rooms	Solid core door (40mm minimum);	
PS45	Communication rooms	Three hinge arrangement; and	
PS46	Communication rooms	Electric strike or mortise lock.	
Electronic Security			
ES01	Security management system	The SMS should govern the electronic access control, intruder and duress alarm, intercom, and CCTV systems throughout the precinct.	

ID	Type	Recommendation	Comment
ES02	Security network	Be segregated from the existing IT network through a secure gateway;	
ES03	Security network	Operate within a VLAN;	
ES04	Security network	Be firewalled from the internet;	
ES05	Security network	Provide device access control measures through IEEE 802.1X or MAC address verification.	
ES06	CCTV functionality	General display of video for ad-hoc security monitoring;	
ES07	CCTV functionality	Control room display for dedicated CCTV operations;	
ES08	CCTV functionality	Simultaneous playback of one or more IP camera video streams;	
ES09	CCTV functionality	Recording of the IP camera video streams, locally (on-site).	
ES10	CCTV Cameras	It is recommended that existing CCTV cameras be replaced as required with digital megapixel CCTV cameras providing a minimum of 1080p resolution	

ID	Type	Recommendation	Comment
ES11	CCTV Cameras	CCTV cameras should be of low profile dome type to reduce visual impact on the precincts architecture.	
ES12	CCTV Cameras	External cameras should be vandal and weather resistant (IK09 and IP66 rating)	
ES13	CCTV Cameras	mounted at a height that reduces the opportunity for human interference	
ES14	CCTV Cameras	External camera fixings and screws should be of marine grade stainless steel	
ES15	CCTV Cameras	Camera housing should be designed to operate in a marine environment.	
ES16	Camera coverage	Building entry/exit points;	
ES17	Camera coverage	Precinct entry/exit points;	
ES18	Camera coverage	Water based entry/exit points to the precinct;	
ES19	Camera coverage	Cafes, restaurants, and bars;	
ES20	Camera coverage	Cash handling areas;	

ID	Type	Recommendation	Comment
ES21	Camera coverage	Lifts;	
ES22	Camera coverage	High value item store entries/exits;	
ES23	Camera coverage	Box office and ticketing areas; and	
ES24	Camera coverage	Future temporary entry/exit points during events held in waterfront Square.	
ES25	CCTV Recording	CCTV footage should be kept to an evidentiary standard, with inbuilt watermark, time and date stamp, as well as clear identification of which camera footage was recorded from	
ES26	CCTV Recording	CCTV image recordings should be stored for 28 days as a minimum.	
ES27	CCTV Recording	CCTV imagery should be stored in a central location within the precinct	
ES28	EACS Functionality	Configurable access zones and sub-zones;	
ES29	EACS Functionality	Anti-pass back controls;	

ID	Type	Recommendation	Comment
ES30	EACS Functionality	Collective controls (groupings of users, zones, access rights etc);	
ES31	EACS Functionality	Configurable access groups comprising users and their access rights to access zones, sub-access zones and individual portals, as well as date / time control;	
ES32	EACS Functionality	Configurable user information;	
ES33	EACS Functionality	Independent intelligent door controllers;	
ES34	EACS Functionality	Manual portal control;	
ES35	EACS Functionality	Interfaces with the CCTV system, fire system, lift system, and other motorised portals;	
ES36	EACS Functionality	Multi technology access cards and compatible readers; and	

ID	Type	Recommendation	Comment
ES37	EACS Functionality	Electric locking and control devices.	
ES38	EACS Architecture	The electronic access control system should be configured with several multi-door controllers, each communicating back to a central access control server	
ES39	EACS Readers	Card readers should be multi-technology (125kHz, 13.56MHz, NFC, and Bluetooth) readers.	
ES40	EACS Readers	Authorised precinct staff and tenants should be provided with their own access card, programed to provide them with access to nominated access controlled portals.	
ES41	EACS Readers	Card readers should be mounted adjacent to the associated portal, on the continuous accessible path of travel, and in clear line of sight of people approaching the portal.	
ES42	EACS Readers	The access cards provided at WBAP should be 13.56Mhz smart cards.	
ES43	Electric Locks	Electric Mortise Locks; for timber single leaf doors, or double doors with the inactive leaf not electrically controlled. Door leaves must be	

ID	Type	Recommendation	Comment
		hinged on the edge (not centrally pivoting, enabling the lock cable to pass cleanly from the frame to the leaf).	
ES44	Electric Locks	Electric Strikes; for fire stair doors, or existing doors where cable access for an electric mortise lock would be otherwise prohibitive.	
ES45	Electric Locks	Electromagnetic Locks; for double doors where both leaves need to be electrically controlled.	
ES46	Electric Locks	Electric drop bolts; It is preferred that these are not used; due to door alignment reliability issues.	
ES47	Electric Locks	All electric locking solutions provided for WBAP should be fail-safe in operation	
ES48	EACS Other Equipment	Request to exit buttons and emergency break glass buttons should be provided to facilitate general or emergency egress through electronic access controlled portals.	
ES49	EACS Other Equipment	Request to exit and emergency break glass buttons should be mounted adjacent to the associated portal, on the continuous accessible path of travel and in clear line of sight of people approaching the portal.	

ID	Type	Recommendation	Comment
ES50	EACS Other Equipment	Request to exit and emergency break glass buttons should comply with and be mounted in accordance with AS 1428.1-2009 – Design for Access and Mobility.	
ES51	Alarm system	Intruder alarm devices should be provided to monitor the integrity of nominated areas.	
ES52	Alarm system	Intruder alarm devices should use the same security control panels as the electronic access control system.	
ES53	Alarm system	The system should comply with AS 2201 – Intruder Alarm Systems.	
ES54	Alarm system	Monitoring, control and administration of the Intruder Alarm and Duress devices should occur at the security monitoring centre.	
ES55	Alarm system monitoring areas	Valuable item/equipment stores;	
ES56	Alarm system monitoring areas	Cash handling areas;	
ES57	Alarm system monitoring areas	Back of house areas outside of operating hours; and	

ID	Type	Recommendation	Comment
ES58	Alarm system monitoring areas	Commercial and office spaces outside of operating hours.	
ES59	Duress and Help Points	Duress alarms should be provided in nominated high risk locations such as cash handling areas, and in accessible toilets.	
ES60	Duress and Help Points	Duress alarm system devices should consist of double push button style duress buttons (non-accessible toilets) that are either wall or under counter mounted.	
ES61	Duress and Help Points	Duress alarms should be latching such that the alarm does not automatically reset until acknowledged and processed at the security control room.	
ES62	Duress and Help Points	The fixed duress alarm system should interface to the IP CCTV system to provide recording and automatic display of camera views of the area in which a duress alarm is initiated.	
ES63	Duress and Help Points	Accessible toilet duress buttons should be of single push, wall mount design.	

ID	Type	Recommendation	Comment
ES64	Duress and Help Points	Upon the activation of a duress device, a priority alarm should indicate the location of the alarm via a graphical display at the security monitoring centre.	
ES65	Duress and Help Points	An emergency help point system should be provided throughout the Precinct	
ES66	Duress and Help Points	Help points should be installed in accordance with AS1428.	
ES67	Duress and Help Points	Help points should be IK09 and IP66 rated for impact and weather resistance.	
ES68	Duress and Help Points	The emergency help point system should operate using digital technology over an IP network	
ES69	Duress and Help Points	Provide clear, undistorted voice communications, free from background noise and external distortion regardless of environmental surroundings; and	
ES70	Duress and Help Points	Ability to automatically display the video from CCTV camera/s viewing the help point at the security control room.	

ID	Type	Recommendation	Comment
ES71	Duress and Help Points	The emergency help point system should have a high level interface with the access control system and the CCTV system.	
ES72	Electronic key control	A suitable electronic key management system should be provided that ensures a single orientation, positive key capture, with electronic access control to the cabinet.	
ES73	Electronic key control	Tamper resistance;	
ES74	Electronic key control	Solid and intruder resistant construction;	
ES75	Electronic key control	Integration with SMS / EACS;	
ES76	Electronic key control	Option for multiple authentication to sign out high security keys (e.g. two person sign out);	
ES77	Electronic key control	Key alarms;	

ID	Type	Recommendation	Comment
ES78	Electronic key control	Maximum key issue per user; and	
ES79	Electronic key control	Electronic Audit Trail.	
ES80	Intercom system	An IP Intercom System should be provided at nominated locations to aid visitor and staff interaction between remote doors	
ES81	Intercom system	Existing intercom systems at WBAP should be upgraded to interface with the security management system, CCTV system, and electronic access control system.	
ES82	Intercom system	Provided intercoms should be installed and mounted in accordance with AS 1428 – Design for Access and Mobility.	
ES83	Intercom system	The IP intercom system should operate using digital technology over an IP network	
ES84	Intercom system	Provide clear, undistorted voice communication, free from background noise and external distortion regardless of environmental surrounding;	

ID	Type	Recommendation	Comment
ES85	Intercom system	Ability to automatically display the video from CCTV camera/s viewing at the Door Station Intercom on nominated Operator Workstations; and	
ES86	Intercom system	Ability to automatically display or highlight the portal associated with the Door Station Intercom when used so the operator can remotely unlock the portal by clicking a master intercom button.	
ES87	Intercom system	The intercom system should have a high level interface with the access control system and the CCTV system	
Security Management			
SM01	Security monitoring centre	A central security monitoring centre (SMC) will be established to manage security for the WBAP and other Arts facilities managed by Arts NSW.	
SM02	Security monitoring centre	The SMC will be coordinated by the Precinct Manager who will be responsible for the smooth, safe and secure operation of the precinct.	
SM03	Security monitoring centre	This may be located at the precinct or outsourced to a third party provider	

ID	Type	Recommendation	Comment
SM04	Security officers	Contract security officers are recommended to be stationed at WBAP at all times	
SM05	Security officers	Security officers should be responsible for responding to alarms, duress, and emergency calls, investigating as required to determine the cause of such events.	
SM06	Security officers	Security officers should be uniformed to be clearly identifiable and visible in the precinct.	
SM07	Training	Security awareness training to be conducted	
SM08	Procedures	List of security procedures to be developed (Section 7.4)	
SM09	Tickets	Tamper evident holograms;	
SM10	Tickets	Gloss marks;	
SM11	Tickets	UV ink;	
SM12	Tickets	Unique barcodes;	

ID	Type	Recommendation	Comment
SM13	Tickets	Security micro text;	
SM14	Tickets	Heat sensitive ticket paper; and	
SM15	Tickets	Electronic tickets.	
SM16	Loading Dock	Loading docks should be controlled areas of the precinct, with deliveries and arrivals monitored at all times.	
SM17	Loading Dock	Vehicles approaching a loading dock should request access from a control point external to the dock	
SM18	Loading Dock	Vehicles should show some form of identification before entry is granted.	
SM19	Loading Dock	Vehicles arriving should, where possible, be scheduled and expected the Precinct Manager.	
Crime Prevention through Environmental Design			

ID	Type	Recommendation	Comment
CP01	CPTED	• Ensure adequate lighting is provided throughout the precinct, particularly at the ends of Wharf 4/5 and Pier 2/3, the precinct and building entry/exit points, and within the waterfront square;	
CP02	CPTED	• Provide way finding signage throughout the precinct to assist natural access control, and reinforce boundaries;	
CP03	CPTED	• Provide security signage throughout the precinct, particularly at precinct and building entry/exit points, to notify people of the security measures in place, and to provide a deterrence;	
CP04	CPTED	• Maintain precinct image and repair vandalism or remove graffiti as quickly as possible (including public seating, shades, etc.);	
CP05	CPTED	• Activate the precinct and the waterfront square as much as possible, to attract legitimate users to the area, and to deter illegitimate users and crime;	
CP06	CPTED	• Use as much glazing as possible to assist natural and electronic surveillance;	
CP07	CPTED	• Support gatherings of community groups throughout the precinct to further activate the space;	

ID	Type	Recommendation	Comment
CP08	CPTED	- Minimise areas of possible concealment of people, actions, or packages, particularly at the ends of Wharf 4/5 and Pier 2/3, staircases, lifts and the northern most and southern most boardwalks.	

Appendix B – Security monitoring centre design

This appendix has been prepared as an example of industry best practice that is consistent with other arts and cultural institutions across Sydney. This appendix will discuss the best practice considerations for a security monitoring centre, whether located onsite or offsite. While the inclusion of a central security monitoring centre (SMC) onsite is considered best practice, an off-site, contract arrangement for security monitoring may be appropriate.

The following advice is important to consider when contracting out security monitoring measures, as well as for designing a local, onsite SMC or security post.

SMC's provide a location to monitor all security information feeds including live monitoring of CCTV cameras, alarm systems, and electronic access control systems. The provision of a central security monitoring centre would be consistent with other cultural institutions in Sydney.

7.6.1 Purpose

The SMC would provide day-to-day operational command and control of the precinct's security strategy. This includes functioning during normal and crisis modes as the primary operations centre. To effectively coordinate operations, the SMC would have precinct wide access to all security systems including CCTV, electronic access control, intruder alarms, and building management systems.

7.6.2 Structural considerations

SMC's are the central hub of security operations during an emergency and crisis situation. This critical operation requires the centre to be target hardened and able to operate in adverse conditions whilst providing a significant barrier to potential intruders or other adversaries. To achieve this aim, several structural considerations should be implemented. These considerations include:

- Having a fire resistant shell, which is also resistant to physical attack,
  - Including an intruder resistant floor-to-soffit perimeter wall constructed of concrete block and/or welded steel mesh.
- The interior of the SMC shall not be visible from the exterior except through electronic means,
- Only having openings into the shell for;
  - Entrance doors,
  - Emergency egress,
  - Ventilation penetrations,
  - Service penetrations,

- Have a maximum of two entrances,
- All doors should open outwards, with a visual identification capability before entrance is granted.

These structural considerations are best practice and provide baseline considerations for the design of a SMC.

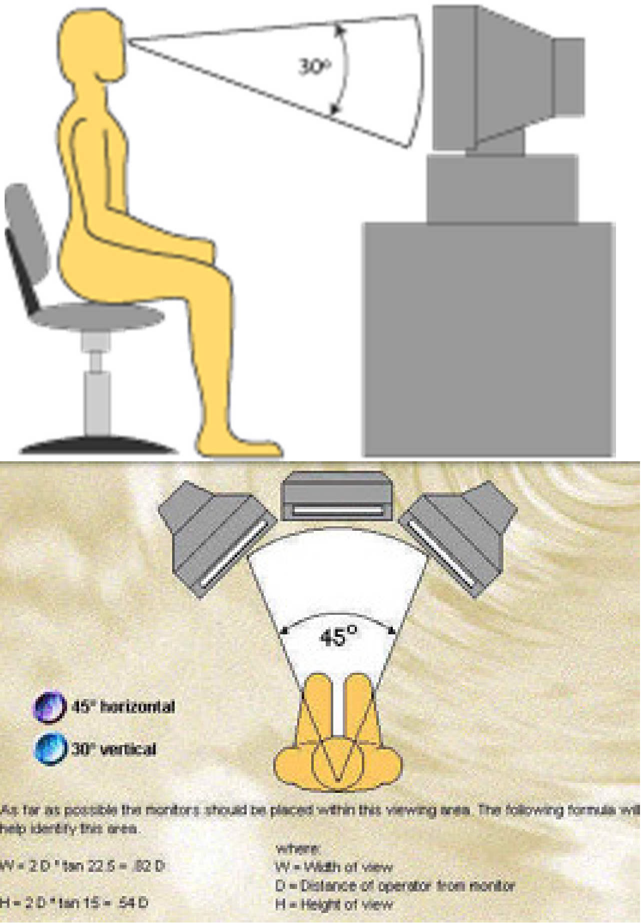
7.6.3 Ergonomic considerations

Security controls rooms are generally operated by staff over long periods of time in shifts. Operators are expected to monitor CCTV imaging systems to ensure the facility is operating as expected, and no security issues have arisen. Furthermore, operators need to be ready to react quickly to potential threats or developing situations on site, and provide a command and control service to roaming guards on patrol. Thus, it is important to consider ergonomic design of the control room to ensure staff remain alert, comfortable, and can operate the room to its full potential in everyday and emergency situations. The following ergonomic features are important in SMC design:

- Architectural factors (including the design and layout of the room itself);
    - Control room operations are restricted if the room is too small, an awkward shape, or contains pillars/sloping ceilings.
    - There must be room for maintenance activities to be undertaken without interrupting regular operations.
    - Ideally, a separate room is allocated for equipment racks, where independent cooling and ventilation systems can be provided.
- Design and layout of individual work stations;
    - The height of desks must accommodate chairs, and numerous seating positions.
    - The workstation depth must be sufficient to hold all equipment, and ensure the operator can write logs, and read documents.
- Arrangement of monitors;
    - Monitors should be placed in easily viewable locations so operators do not crane their necks.
    - Monitors must be of sufficient size for detail to be seen from the workstation, as a general rule, operators should be at least twice the distance from the screen as the height of the display, and at most eight times the height.
    - Primary viewing monitors should be located within a 30° vertical, 40° horizontal viewing cone.
- Design of control systems;

  - All work materials and equipment must be located within reach of the operator to ensure efficiency of use and reduce fatigue.

- Seating;
  - An ergonomically designed operator chair must be provided.
  - Seating must have adjustable height, backrests, arm rests, foot rests, and support good seating posture.
- Environmental factors (including heating, lighting and ventilation);
  - Lighting should be diffuse and arranged in such a way as to avoid glare from monitors or displays.
  - HVAC systems should provide a comfortable working temperature all times of the day, and provide fresh air.
  - Extraneous ambient noise from telecommunications racks and servers should be kept at a minimum.
- Accessibility for disabled staff and escorted visitors.



As far as possible the monitors should be placed within this viewing area. The following formula will help identify this area.

W = 2 D * tan 22.5 = .82 D

H = 2 D * tan 15 = .54 D

where:
W = Width of view
D = Distance of operator from monitor
H = Height of view

Figure 18. Ergonomic considerations

7.6.4 Entry considerations

The SMC should have an electronically controlled entry door with read-in functionality. This access control entry point should be restricted to those users who have a valid ‘*need-to-go’* only, such as security, key facilities staff and certain management personnel. Visitors to the site such as service technicians would present themselves to the door, and communicate through an intercom system. This intercom system would provide video-identification of the visitor before access is granted by an operator.

7.6.5 Work stations

In general, SMC work stations are provided for distinct building management tasks. These stations include video monitoring and control systems, building management control systems, incident management systems, intruder detection systems, and electronic access control systems. To effectively operate and monitor such systems, it is considered good practice to provide a multi-head display for each work station.

Furthermore, supervisor work stations are generally installed in SMC’s to ensure staff remain accountable and able to quickly action tasks which require supervisor approval. The supervisor work station is generally positioned behind operator work stations to provide a visual line of sight. This work station is ideally supplemented by one spare hot desk for use in emergency situations.

In addition, high stress and crisis situations can cause operators to have trouble accurately using a keyboard and mouse input configuration. Best practice dictates the use of a dedicated CCTV control device with joystick, or touchscreen interface.

Each work station should have the required space for:

- A slimline, high performance workstation PC,
- Multi-monitor displays,
- Standard keyboard and mouse input,
- CCTV operator keyboard,
- Ergonomic seating; and
- Operator telephone and intercom master station.

The hot desk shall have space for:

- Ergonomic seating; and
- Operator telephone.

7.6.6 Lighting and HVAC

The SMC should be designed to reduce operator irritability and fatigue wherever practicable. This shall include the installation of a HVAC system to control temperature and airflow, as well as diffused, dimmable LED strip lighting. The HVAC system should provide fresh air circulation at a controlled temperature 24/7 to suit operational needs. The strip lighting should illuminate the entire space sufficiently so that no shadows are cast over operator work stations when in use, while ensuring all monitors and displays do not produce glare or reflect light.

7.6.7 Card printing

The proposed SMC would centralise security operations within the precinct, and as such, should be capable of providing a full security service offering. Card printing and photo identification issuing is an important task undertaken by security personnel. This task requires operators to have access to a card printer, digital camera, flash lighting equipment and retractable backdrop.

Figure 19. Example card printer

7.6.8 Video monitoring wall

The SMC would be the central hub of control for all security and emergency events on the premises. This requires extensive information to be displayed to operate effectively during day to day tasks and crisis situations. It is important for all staff within the SMC to have a continuous live feed of CCTV systems around the facility for continuous review and monitoring. Generally, due to the number of cameras inherent in a precinct as large as WBAP, several video displays would be required to effectively view important camera feeds concurrently.

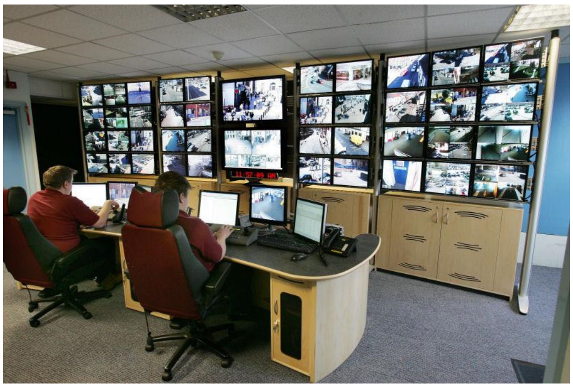


Figure 20. Example video wall

7.6.9 Connectivity and power

Ideally, the SMC should have the means for direct communication to the police so that immediate contact can be made in times of emergency or during incidents. The control room should have at least two independent means of external communication. Due to the number of services the SMC will be required to monitor and review, extensive network access should be provided to ensure effective operation.

This network access should be future proofed, as increasing services at a later date would be costly and inefficient. The inclusion of high bandwidth services such as multi-mode fibre cabling in excess of proposed requirements is recommended.

7.6.10 Radio dock stations

As an operations hub, the SMC should have facilities in place for efficient, ease of use. Security operations staff require easy access to radios and charging stations throughout their work shifts, and it would be beneficial for the SMC to have a waist height radio dock station to facilitate this. In consideration of best practice and other SMC designs within the Sydney CBD, the inclusion of a radio dock station near the airlock is generally preferred.

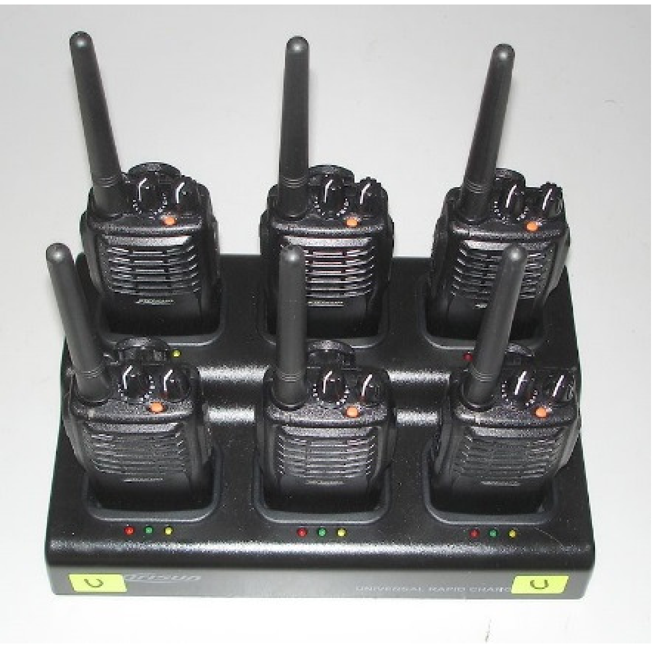


Figure 21. Example radio dock station

7.6.11 Amenities and facilities

Staff working in an SMC are generally expected to work for long shifts and provide ongoing monitoring of all security systems and CCTV camera feeds throughout this time. Therefore, consideration must be given to change rooms, bathrooms, and other essential facilities such as kitchenettes to ensure staff can remain within the SMC throughout the extent of their shift. Furthermore, the inclusion of changing facilities provides security operations staff the ability to store uniforms, utility belts, and other equipment in a secure area after work hours.