

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

Fusion Project Management
102-108 Jeffcott Street
Post-Construction Security
Requirements

Issue 03 | 1 February 2021

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 276557-00

Arup Pty Ltd ABN 18 000 966 165

Arup
Sky Park, One Melbourne Quarter
699 Collins Street
Docklands
VIC 3008
Australia
www.arup.com

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

Document verification

Job title		102-108 Jeffcott Street		Job number 276557-00	
Document title		Post-Construction Security Requirements		File reference	
Document ref					
Revision	Date	Filename	201201 – Post-Construction Security Requirements Issue 01		
Issue 01	01 Dec 2020	Description			
			Prepared by	Checked by	Approved by
		Name	Aaron Lillis	Luke Pascoe	Luke Pascoe
		Signature			
Issue 02	18 Jan 2021	Filename	210118 – Post-Construction Security Requirements Issue 02		
		Description			
			Prepared by	Checked by	Approved by
		Name	Aaron Lillis	Luke Pascoe	Luke Pascoe
Signature					
Issue 03	01 Feb 2021	Filename	210201 – Post-Construction Security Requirements Issue 03		
		Description	Final issue – incorporated updated drawings		
			Prepared by	Checked by	Approved by
		Name	Aaron Lillis	Luke Pascoe	Luke Pascoe
Signature					

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

Contents

	Page
1 Introduction	1
2 Security Planning Requirements	1
3 Stakeholder Engagement	2
4 Threats	3
5 Security Management Plan	4
5.1 Monitoring & Managing Rooftop Access	4
5.2 Maintenance & Contractor Approvals	7
5.3 Restricting Overlooking & Recording of the MAP	8
5.4 Incident Reporting	9
6 Conclusion	10

Appendices

Appendix A

Physical Security Specifications

Appendix B

Incident Reporting

This copied document to be made available for the sole purpose of making its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

1 Introduction

Arup has been engaged by Fusion Project Management to provide security consulting services for the 102-108 Jeffcott Street residential development. As part of this scope of services, the following has been undertaken:

- A meeting with a Department of Justice and Community Safety (DJCS) representative to determine the DJCS interpretation of security requirements imposed on the development;
- Development of a construction phase security management plan identifying specific controls for the contractor to implement relating to the presence of the Melbourne Assessment Prison (MAP) across the road from the development
- Development of an operations phase (post construction) security management plan to address the security planning requirements (this report).

This report contains security control guidance relating to the development *post-construction*.

2 Security Planning Requirements

Due to the development’s proximity to the MAP, security-related planning requirements have been imposed on the development for post-construction. These requirements are detailed in Table 1.

Table 1 Operations Phase requirements

Reference Section	Requirement
1. c)	Integrated permanent design treatment(s) in accordance with the plan prepared by Hachem SK119 (Rev. 4, dated 9/10/19) to the southern elevation of levels 9 and above (excluding the roof level) of the building at 102-108 Jeffcott Street (“the Jeffcott Street building”) to prevent views of the outdoor recreation areas of the Melbourne Assessment Prison.
11.b)	For use and operation of the Jeffcott Street building: <ul style="list-style-type: none"> i. Ensure that access to the rooftop level is only available to approved personnel that require access to the rooftop for maintenance or operational purposes. The approved personnel must complete a site induction program and follow procedures to avoid and minimise risks and potential impacts on the operation of the Melbourne Assessment Prison; ii. Ensure that access to the rooftop level is only available through a secure door under management supervision; iii. Maintain a logbook to record all access to the rooftop, a copy of which must be produced to the Department of Justice and Community Safety upon written request.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright.

3 Stakeholder Engagement

Arup has engaged with the Department of Justice and Community Safety (DJCS) in two workshops.

Workshop 1 – 24th July 2020 1:00-2:00PM

Attendance: Gavin Blair (General Manager MAP), Luke Pascoe (Arup), Aaron Lillis (Arup)

Purpose/ Outcomes:

- Undertake a threat identification exercise
- Discuss and identify perceived threats to the MAP by the development and
- Appropriateness of preliminary control recommendations.

A threat list was developed and concerns around construction impact to MAP operations were also raised.

Workshop 2 – 27th November 2020 1:00-2:00PM

Attendance: Gavin Blair (General Manager MAP), Ian Hughes (Maintenance Manager MAP), Gareth Day (Security Operations Manager, MAP), Luke Pascoe (Arup), Tegan Stott (Fusion Project Management), Aaron Lillis (Arup).

Purpose/ Outcomes:

- Engage with the DJCS on controls and mitigation strategies to be deployed to address the identified risks and planning requirements.

The proposed controls were workshopped with the MAP and agreement achieved that the controls address the identified risks. Additional risk scenarios were identified, however the proposed controls were deemed sufficient to address risks originating from the development. The need for ongoing communication was noted and agreed between the project team and DJCS.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

4 Threats

As noted, a threat identification exercise was undertaken with the DJCS (24th July 2020) to understand the potential security threats underlying the planning requirements (associated with its proximity the MAP). Threats identified as applicable to the site post-construction are captured in Table 2 below.

Table 2: Identified threats (DJCS)

Threat	Comments
Recording/ Photographing prison operations and persons in custody from rooftop and upper levels	Higher levels (Level 9 and above) overlook the prison recreation yard. DJCS are concerned about potential overlooking/ recording of these areas.
Throwing contraband into the MAP yard	The height of the development presents opportunities to throw prohibited items into the MAP yard (e.g. drugs, tools, weapons etc.) from the rooftop/ balconies. DJCS also raised concerns relating to use of tennis racquet to hit tennis balls filled with contraband into MAP areas.

Controls have been proposed (see Section 5) to reduce the above identified risks.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

5 Security Management Plan

Strategies identified to mitigate the identified threats and to contribute to the development meeting its security-related planning requirements have been split into four overarching categories:

- Monitoring / management of rooftop access;
- Maintenance and contractor approvals;
- Restricting overlooking/ recording of the MAP;
- Incident reporting/ record keeping.

5.1 Monitoring & Managing Rooftop Access

5.1.1 Performance Criteria

Security controls (including CCTV and access control measures) shall be implemented to restrict access to the rooftop plant areas to authorised personnel (refer to Section 5.2), to detect unauthorised access and to record footage for evidentiary purposes.

5.1.2 CCTV

Summary of Requirements

- CCTV coverage of all access points to the rooftop (with recording & storage capabilities) at **identification grade** coverage.

CCTV coverage is proposed to meet the following performance criteria:

- CCTV is to be implemented at all rooftop access doors to facilitate the identification of those accessing the rooftop;
- CCTV recordings shall be retained for traceability (see specification);
- Coverage is to meet an **identification grade** for rooftop access.

CCTV specifications are provided in Appendix A.

5.1.3 Access Control (Electronic & Mechanical)

Summary of Requirements

- All access doors to the plant area and common areas of the rooftop shall have access control systems implemented to prevent unauthorised access;
- The plant area shall include an intrusion detection system;
- Design to include robust access doors for the rooftop;

This copied document to be made available for the sole purpose of making its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

Building security and management shall implement access management policies and procedures;

- Intercoms within plant area rooftop for OH&S purposes.

To facilitate the restriction of access to authorised persons/ residents only to rooftop areas, access control measures are proposed.

Requirements for Rooftop Access Doors to Plant Area

Performance and technical requirements, detailed in Appendix A, include:

- Electronic Access Control Systems (EACS);
- Intrusion Detection Systems (IDS); and
- Robust door hardware (for rooftop access door).

These systems in combination with CCTV will allow for the recording and detection of unauthorised access to the rooftop plant area.

Note: To fulfil the requirement to provide a log of all access to the rooftop, it is proposed that electronic access systems are implemented for the **common area** that are capable of logging access times against unique user identification for each person with approved access (e.g. key card or unique access code).

Door Construction

- For robustness, rooftop access doors to be designed as a minimum 60-minute fire door (subject to fire life safety requirements) – including associated door frame.

Door Locking Hardware (Mechanical) – If Used

- Comply with AS 4145.1 and AS 4145.2. Mechanical locks shall achieve (as a minimum):
 - Lockset: SL3
 - Cylinder: SC3
 - Lock: S3
 - Keying: K3
 - Durability: D-

Electronic Locking Mechanisms

- Comply with the electronic access control specification (detailed in Appendix A)
- Must be designed to fail “safe”.

5.1.4 Granting/Removing Access

Building security and staff shall comply with written operational processes and policies to grant or remove access privileges to the rooftop areas.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which breaches any copyright

Operational processes shall include a written policy for all staff that addresses:

- Who shall grant access;
- To whom access shall be granted;
- How access is granted (including providing supervision);
- Site induction requirements (for maintenance/ contractor access);
- Documentation of permitted access;
- Incident reporting mechanisms, and;
- Processes for revoking access permissions for residents and staff no longer requiring access.

5.1.5 Intercom System (OH&S)

For Occupational Health & Safety purposes, an intercom system is proposed to be fitted at the exterior of rooftop access doors to alert building management should someone be locked/ stuck outside or in the event of an emergency.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright.

5.2 Maintenance & Contractor Approvals

Summary of Requirements

- Logbook recording all approved access to the plant area of the rooftop;
- Site induction – including rules and expectations related to the MAP.

5.2.1 Performance Criteria

Building management shall implement policies and procedures to induct contractors/ maintenance workers and monitor access to the rooftop plant area for the purposes of supporting the DJCS in identifying people following a security incident.

5.2.2 Requirements

Induction Requirements

Building management shall implement induction programmes that include the following:

- Verification of identity – including an ID check (driver’s license or equivalent);

In addition, the induction process shall communicate security-specific code of conduct, including:

- No filming/ photography at the rooftop level without permission;
- No drones permitted on site (without prior permission, subject to CASA approvals);
- Sign in requirements (each visit, in the logbook);
- Access policies (return of key or access card as applicable at the end of the visit).

Logbook

Building management shall maintain a logbook of visitors accessing the **plant area** of the rooftop, including the following minimum details:

- Full name;
- Role/ organisation;
- Access purpose;
- Telephone contact details.

Consistent with the induction requirements, building management is to request ID for the first time the contractor visits the site to verify the identity of visitors.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which infringes this copyright.

Note that this information is required to be provided to the DJCS on request in order to fulfil planning requirement 11.b) iii (see Section 2).

*Note that as with construction phase requirements, logbooks may be facilitated through a digital equivalent provided it is capable of capturing the required information.

5.3 Restricting Overlooking & Recording of the MAP

5.3.1 Performance Criteria

The design is to restrict views and the capability of individuals to record MAP and its operations from levels 9 and above.

5.3.2 Design Response

An architectural solution to restrict the capability of building occupants to view/record footage of the overlooking area has been implemented for the south-facing edge of the building façade from Level 9 and above. This façade treatment (shown in Figure 1) consists of proprietary glazing with internal timber louvers angle upwards at 30° to restrict the field of view through glazing (preventing looking downward).

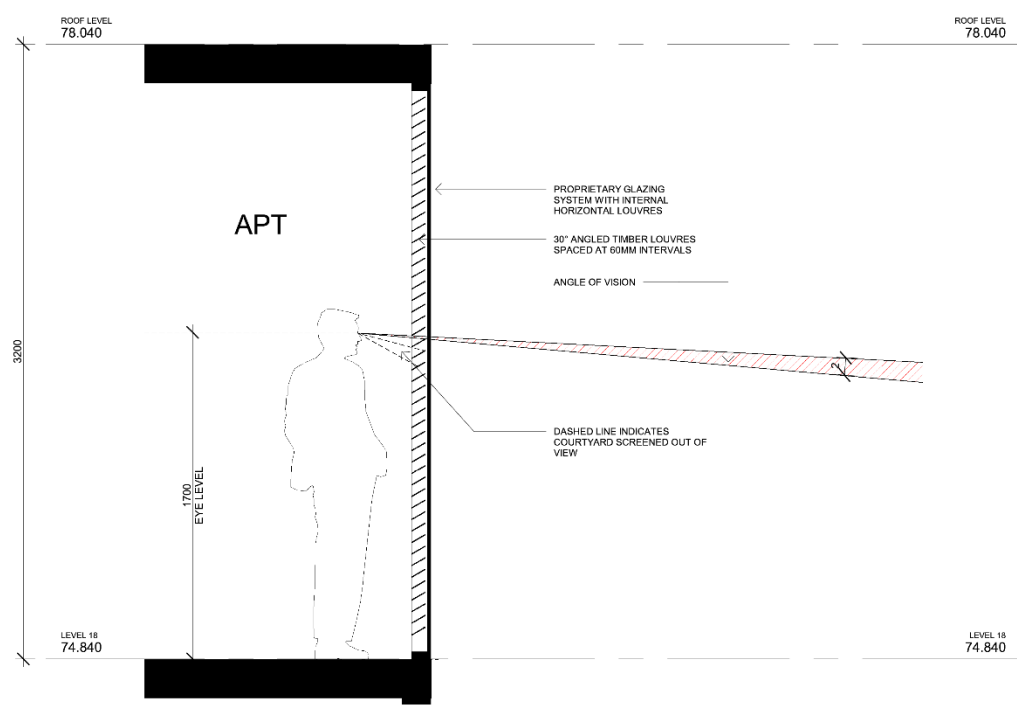


Figure 1 Façade treatment (apartment views towards MAP)

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

5.3.3 Rooftop/ Common Areas

While rooftop access is proposed to be restricted to plant areas current plans include provision of a common area on the rooftop. To restrict the overlook into the MAP, the façade treatment (level 9 and above on the southern facing façade) has been extended to the rooftop area. Additionally, the area closest to the southern side is a covered area, restricting the capability of individuals to throw contraband into the prison from the rooftop (a threat identified during the workshop with DJCS). It is noted that these controls are in addition to the proposed access management strategies and CCTV provisions for the rooftop.

Note: Access to the plant area is to be restricted and subject to the proposed access management strategy highlighted in sections 5.1 and 5.2.



Figure 2 Southern extent of rooftop – covered dining area

5.4 Incident Reporting

Building security and management shall implement processes and policies for the reporting of security-related incidents on the rooftop. As a minimum, this is expected to include the following to comply with the Development’s planning requirements:

- Unauthorised access to the rooftop;
- Suspicious behaviour on the rooftop or at rooftop access points;
- Damage to the rooftop door;
- Damage to access control systems.

It is noted that these relate solely to the requirements related to the MAP and is not intended to reflect an exhaustive list. There may be other security incidents that warrant reporting subject to the Building Manager’s policies and procedures.

This copied document to be made available for the sole purpose of making its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which infringes any copyright.

An example incident report document is provided in Appendix B.

6 Conclusion

As noted in section 2, the development’s proximity to the MAP, specific security-related planning requirements must be addressed for post-construction. Security requirements proposed to address the planning requirements and the threats identified with DJCS are summarised in Table 3 below.

Table 3: Summary of requirements

Requirement	Control
Management of Common Areas & Residential Exterior	<ul style="list-style-type: none"> ● CCTV of common areas on rooftop; ● Electronic access to authorised residents.
Monitoring and Managing Rooftop Access	<p><u>Electronic & Mechanical</u></p> <ul style="list-style-type: none"> ● CCTV; ● Access Control (Electronic and/or Mechanical); <ul style="list-style-type: none"> ○ Electronic Access Control Systems (EACS); ○ Intrusion Detection Systems (IDS); and ○ Attack resistant door hardware (for rooftop access door). ● Intercom (exterior side). <p><u>Operational</u></p> <p>Written operational processes and policies to include:</p> <ul style="list-style-type: none"> ● Granting or remove access privileges; ● Logbook of authorised & unauthorised access; ● Induction of maintenance & contractors; ● Incident Reporting.
Restricting Overlooking & Recording of the MAP	<ul style="list-style-type: none"> ● Proprietary glazing system with internal timber louvers angled to 30° ● Common area on the side of the rooftop closest to the MAP is covered and façade treatment extended to the rooftop level (southern side).
Incident Reporting	<ul style="list-style-type: none"> ● Incident documentation and reporting to DJCS.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

**ADVERTISED
PLAN**

Appendix A

Physical Security Specifications

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

A1 CCTV

Internal fixed cameras shall all be colour units with the following features:

- Resolution: minimum 1920 x 1080 pixels;
- Video streaming: Multi-cast; multi-streams (a minimum of 3 streams);
- Video compression format: H.264 or H.265 format;
- Sensor: CMOS, progressive scan;
- Day/light capability. The switching between modes is user configurable to be set to auto or manual;
- Minimum illumination: Colour – 2.3 lux;
- Camera angle adjustment: Pan 3600, Tilt 1700, Rotation 3400;
- Maximum frame rate: 30 fps H.264/MPEG-4 at 1080p;
- Support SDXC up to 128GB for local alarm recording;
- Power: PoE (class 1) or 12 VDC;
- Auto-iris;
- Varifocal lens;
- Supported protocols: IPv4/v6, HTTP, HTTPS, FTP, SMTP, NTP, RTSP, RTP, TCP, UDP, SNMP;
- Backlight compensation;
- White balance;
- Automatic gain control;
- Wide dynamic range of at least 57 dB;
- Vandal resistant;
- IP45 rated;
- Tamper alarm;
- Integrated with IR illuminator. The IR illuminator shall have a minimum of 20 metres range;
- ONVIF compliance;
- Interface – 10BaseT/100Base-TX (RJ45), 1 x analogue monitor output (BNC), 1 x sensor input and 1 x alarm output (24V AC/DC, 1A).

The internal camera unit shall be miniature dome or standard in form. Housings shall be in a form and colour approved by the Architect. If dome cameras are proposed, dome cover shall come with optional smoked colours for selection.

Where internal dome cameras are supplied, they shall wherever possible be drop-centring mounted, and where standard form cameras are supplied, the associated bracket shall be of a form and colour approved by the Architect.

External fixed cameras shall be colour true day/light changeover units with the following features:

- Resolution: minimum 1920 x 1080 pixels;
- Video streaming: multi-cast; multi-streams (a minimum of 3 streams);
- Video compression format: H.264 or H2.65 format;
- Sensor: CMOS, progressive scan;
- Day/light capability. The switching between modes is user configurable to be set to auto or manual;
- Minimum illumination: Colour – 2.3 lux;
- Camera angle adjustment: Pan 3600, Tilt 1700, Rotation 3400;
- Maximum frame rate: 30 fps H.264/MPEG-4 at 1080p;
- Support SDXC up to 128GB for local alarm recording;
- Power: PoE or 12 VDC;
- Auto-iris;
- Supported protocols: IPv4/v6, HTTP, HTTPS, FTP, SMTP, NTP, RTSP, RTP, TCP, UDP, SNMP;
- Varifocal lens;
- Minimum object distance: 300mm;
- Backlight compensation;
- White balance;
- Automatic gain control;
- Wide dynamic range of at least 57 dB;
- ONVIF compliance;
- Vandal resistant;
- Tamper alarm;
- Integrated with IR illuminator. The IR illuminator shall have a minimum of 20 metres range;
- Housing: IP 66 rated and IK10;
- Interface – 10BaseT/100Base-TX (RJ45), 1 x analogue monitor output (BNC), 1 x sensor input and 1 x alarm output (24V AC/DC, 1A).

The external camera unit shall be miniature dome or standard in form. Housings shall be powder-coated and shall come with sun shroud and heater to avoid misting and condensation of water vapours within the housings. Housings shall be

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright.

the dome cover shall come with optional smoked colour for selection. approved by the Architect. If dome cameras are proposed,

Where standard form cameras are supplied, the associated bracket shall be of a form and colour approved by the Architect.

It should be noted the security contractor is responsible to select the most appropriate lens type with the correct focal length (2.0 – 50.0mm) to meet the operational requirements of the cameras.

In accordance with the actual site situation, select the most appropriate mounting method, tamper-proof mounting screws and accessories. The proposed mounting method and accessories shall be submitted to the Architect and design consultants for approval before procurement.

Operational Performance	Description	Min Screen Height %	Pixels / m
Facial Identification (FI)	Use of the video or still image for positive identification of an individual, for the purposes of supporting an investigation or prosecution. Given a comparative image of equal quality of a known individual, identification must be beyond reasonable.	100	250
Facial Recognition (FR)	Use of the video or still image to support recognition of an individual for the purposes of supporting an investigation. A viewer of the image can say with a high degree of certainty that the individual is, or is not, someone they have seen before.	50	125
Activity Observation (AO)	Use of the video to observe, with a high degree of reliability, the nature of the activity within the field of view.	25	62
Presence Detection (PD)	Use of the video to establish, with a high degree of certainty, the number, direction and speed of movement of people (or vehicles) within the field of view.	10	25
Area Monitoring (AM)	Use of the video for live view routine maintenance of crowds and locations.	5	12

Video recording shall be capable of meeting the following requirements:

- Rack-mountable (to be located in ground floor Communications/Server room);

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright.

- H.264 or H.265 compression;
- 30 days (4 weeks) minimum recording capacity at 30 fps for all cameras (i.e. worst case scenario);
- Disk array with hot swappable disks;
- Raid 5 configuration;
- Support multiple screen display, e.g. full screen, 4 / 6 / 8 / 9 / 12 / 16 cameras displays;
- Support hot standby dual redundant servers;
- Support clients-servers configuration;
- Flexible bandwidth management – the VMS must be capable to adjust the bandwidth required for streaming video images for each camera based on the amount of activities capture the camera;
- Support multiple transmission technologies such as fibre optic cable and Cat6 cable;
- Support quick search (by time, date and events) of recorded images;
- Live images will automatically pop up on screen when an alarm is triggered. At the same time, the frame rate will automatically increase to 30 fps;
- Export recorded images to external media such as USB drives and CD's;
- Support web-based service;
- Support mobile applications including Apple and Android;
- ONVIF compliant;
- Support communications with remote servers or remote viewing clients via LAN / WAN connectivity;
- Recorded images will be stamped with 'watermark'. Alteration to recorded images will generate alarm when the altered images are replayed.
- Capable to support an additional camera by adding additional licences to the system without major modification or upgrade to the CCTV system front-end required.

A2 Electronic Access Control Systems

Equipment	Specification
Card Reader	<ul style="list-style-type: none"> • Proximity Smart Card type; • Vandal resistant and fixed with tamper resistant screws; • Robust and of a neat, slimline aesthetic profile (suitable for mullion mounting). Selectable style and colour. Units that match the décor of the surroundings are preferable;

This copied document to be made available for the sole purpose of making its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

	<ul style="list-style-type: none"> ● Sealed against any contamination to at least IP66; ● Provide audible and visual indication (tri-colour) of a valid, invalid and faulty card read; ● Minimum “read” range to be 120mm; ● Mounted with tamper resistant fixings in external areas; ● Operating temp. -20°C ~ +55°C; ● Readers must provide a monitored “pulse” signal to the controller to help identify lost communications; ● Generally, the centreline of the access reader to equal the centreline of the lock/latch assembly for the associated door; ● Card Reader shall be HID or approved equivalent.
Access Card	<ul style="list-style-type: none"> ● Be encrypted with a minimum DESFire EV2; ● Be 13.56MHZ type, meeting ISO 15693, 7810 and 14443 for contact-less communications; ● Be provided with site code and security “key” that are unique to the project; ● Have all licenses and authorisations in the name of the Client; ● Incorporate read/write memory (minimum 8K) for the secure storage of data; and ● Be capable of being directly printed on to both sides (e.g. card holder’s name, photograph, etc).
Electronic Mortise Lock	<ul style="list-style-type: none"> ● 12Vdc- 24Vdc Operating Voltage; ● Monitoring: <ul style="list-style-type: none"> ○ Dual key override deadlatched ○ Locked ○ Door closed ○ Request to exit ● Operational temperature range -20c to + 60c; ● High purity zinc alloy construction with stainless steel plates and latchbolts; ● Standard Lockwood oval shaped cylinders; ● 1.6m cabling.
Reed Switch	<ul style="list-style-type: none"> ● Door forced/door open too long alarm; ● Dry relay contacts, closed when door is fully closed; ● Door gap tolerance of <=10mm;

This copied document to be made available for the sole purpose of making its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

	<ul style="list-style-type: none"> • Hermetically sealed, nylon cased; • Built in end of line resistors.
Failure Mode	<ul style="list-style-type: none"> • Access system is to be designed to fail “safe”

A3 Intrusion Detection

System components include but shall not necessarily be limited to the following:

- Control and communications equipment;
- Data gathering panels;
- Intrusion detection devices;
- Tamper circuit monitoring;
- Arming station(s);
- Battery backup and power supply;
- Interface to lighting controls.

A4 Audio Intercom

Performance	Description
Audio streaming	Two-way, Full duplex
Audio compression	AAC LC 8/16 kHz, G.711 PCM 8 kHz, G.726 ADPCM 8kHz, Configurable bit rate
Audio output	85 dB (at 0.5 m)
Audio input/output	Line output, Built-in microphone, Built-in speaker
Video streaming	Multi-cast; multi-streams (a minimum of 3 streams)
Echo cancellation	Yes
Noise reduction	Yes

A5 Door Hardware

To deter and delay threat actors, door hardware to rooftop access doors shall meet the following minimum requirements:

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which infringes any copyright.

- Door to be designed as a minimum, commensurate to a 60-minute fire door (subject to fire life safety requirements) – including associated door frame.

Mechanical Door Locking Hardware

- Comply with AS 4145.1 and AS 4145.2. Mechanical locks shall achieve (as a minimum):
 - Lockset: SL3
 - Cylinder: SC3
 - Lock: S3
 - Keying: K3
 - Durability: D-

Electronic Access Control Systems

Meet the electronic access control specification requirements detailed in Section A2.

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

**ADVERTISED
PLAN**

Appendix B

Incident Reporting

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

B1 Example Incident Report Form

Details of the person completing this form	
Name:	
Contact phone number:	
Email:	

Incident Details	
Time and Date of incident:	_____ : _____ am/pm on ___/___/___
Location:	
Brief description of incident:	
Activity being undertaken (if applicable):	
Names & contact details for witness of incident (if any):	
Was anyone injured:	<input type="checkbox"/> Yes <input type="checkbox"/> No How many: _____

Incidents of unauthorised entry	
Details of unauthorised entry/trespass	

This copied document to be made available for the sole purpose of enabling its consideration and review as part of a planning process under the Planning and Environment Act 1987. The document must not be used for any purpose which may breach any copyright

What action was taken in response to the incident:	
What preventative action should be taken to prevent similar incidents in the future:	
Were authorities notified:	<input type="checkbox"/> Yes <input type="checkbox"/> No
Is this incident required to be reported to the Department of Justice and Community Safety:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/>