



MACQUARIE
University
SYDNEY · AUSTRALIA

Electronic Security Access Control Master Specification

Version: 1.3: March 2019

VERSION CONTROL

Version	Date	Author	Amendment	Distribution
1.0	08/12/2018	S Myles		1 st Draft
1.1	11/12/20108	A Buckton	Review	Internal
1.2	12/12/2018	S Myles	Release	Client Review
1.3	30/03/2019	S Myles	Help Points	Client Review

Table of Contents

1	Introduction	5
1.1	General.....	5
2	Scope	6
2.1	General.....	6
2.2	Performance Objectives	6
2.3	Standards	7
3	Design Parameters	7
3.1	Other Requirements.....	8
3.1.1	Equipment Radio Frequency Interference	8
3.1.2	Equipment Electromagnetic Compatibility	8
3.1.3	Energy Conservation.....	8
3.1.4	Life Cycle Costs	8
3.1.5	Expansion.....	8
4	Alternate Equipment	9
5	Project Obligations.....	9
5.1	'As Installed' Drawings	9
5.2	Operational and Maintenance Manuals	10
5.3	Template	10
6	Compliance and Statement.....	11
6.1	General.....	11
6.2	Statement.....	11
7	Glossary	12
8	Technical Requirements	13
8.1	Door Hardware	13
8.1.1	Electronic Mortice Lock	13
8.1.2	Electronic Door Strike	14
8.1.3	Pre-load Pressurized Doors (Harsh Environments).....	14
8.1.4	Electromagnetic Locks	15
8.1.5	Integrated Wireless Mechanisms.....	15
8.1.6	Integrated Door Wireless Communication Hub.....	17
8.1.7	Movement Detectors	17
8.1.8	Reed Switches	18
8.1.9	Request to Exit (REX) Button.....	18
8.1.10	Duress Alarms.....	19
8.1.11	Desk Mounted Duress Switch.....	19
8.1.12	Wall Mounted Duress Switch (Heavy Duty).....	19
8.1.13	Call Point Emergency Break Glass Unit (BGU).....	20
8.1.14	Card Readers.....	20
8.1.15	Pin Card Readers.....	22
8.1.16	Intelligent Field (Door) Controller (IFC).....	22

9	Access Control System Requirements	27
9.1	Door Control	27
9.1.1	Reception access general:.....	27
9.1.2	Egress control	27
9.1.3	Door Operation Monitoring Recording	27
10	Door Register.....	28
11	Uninterruptable Power Supply Units (UPS).....	29
11.1	General UPS Requirements.....	29
11.1.1	UPS Batteries.....	30
12	Contractor Requirements	30
13	Power	31
14	Cabling	31
14.1	CAT 6 Specifications	32
15	Conduit and Ducting	32
15.1	Conduits	32
15.2	Steel Conduit.....	33
15.3	Rigid UPVC Conduit.....	33
15.3.1	UV Resistant UPVC Conduit.....	33
15.4	Flexible Conduit	33
15.5	Ducting	33
16	Fixings to Walls.....	33
17	Fastening.....	34
18	Penetrations.....	34
19	Make Good & Clean Up	35
19.1	Debris	35
20	Labelling	35
21	Equipment Enclosures	36
22	Fire Rating and Safety	36
23	Workmanship.....	36
24	Licences Certifications	36
24.1	Security Licences	36
24.2	Other Licences and Certifications	36
25	Health and Safety	36
26	Warranty	37
27	Maintenance	37
28	Drawings and Manuals.....	37
29	Commissioning and Acceptance testing.....	38
30	Training.....	38
31	Safety & Environment	38
32	Instructions:	39

1 Introduction

Macquarie University's Electronic Security and Access Control, Integrated Security Management Solution (ISMS) Master Specification is designed to provide potential contractors with all the necessary information required to complete the detailed design, procurement and implementation of the required systems within its Campus and building locations.

The development of this Specification is based on available standards and principles of recognised best practice. References are made to Australian and International Standards where the application of these is deemed appropriate.

The existing ISMS head end system is Gallagher, as such the intent of this document is to allow Contractors to align their responses with requirements of additional works stipulated within supporting design documents and subsequent site drawings.

1.1 General

The Master Specification when used in conjunction with the design brief and supporting drawings, shall provide potential Contractors with all the necessary information for a fully functional, cost-effective installation of finished works that comply with Macquarie University's (MQU) requirements.

The Contractor as part of their submission is required to provide a design including all workshop drawings for a finished system that complies with the Specification, including, however not limited to the installation, commissioning, and 12 Months Defects Liability and Preventative Maintenance.

The solution shall provide a means to control access through nominated doors throughout the University. The solution shall include as a minimum electric locking door status monitoring and token or biometric access control readers. Access rights associated with a presented access token or biometric identifier shall be checked for validity based on token or identifier, access area, access time and any other access management function defined in this specification.

All access data shall be stored in intelligent field controllers and access shall be granted or denied dependant on user privileges. Access rights shall be programmed in a variety of ways to allow flexibility as defined within this specification.

The Contractor shall as a minimum in conjunction with MQU Stakeholders install, connect and make good the following;

- i. Access control;
- ii. Alarms management;
- iii. Cardholder management;
- iv. CCTV integration;
- v. Integrated Visitor Management;
- vi. Help Point Intercom Integration
- vii. Guard Tour;
- viii. Perimeter deterrent and detection integration.

The Contractor shall provision and install all required infrastructure so that Macquarie University are provided with a complete cost-effective installation of finished works thoroughly tested and ready for operation.

The Contractor shall provide all the required infrastructure to interface with the University's existing Gallagher Security System and run all new cables including those to the nominated demarcation points within the campus. The security contractor will liaise with the University's authorised person to agree and finalise all demarcation points prior to the commencement of scheduled works.

2 Scope

2.1 General

This specification sets out the equipment and materials to be used and installation methods employed in the provisioning of Electronic Security and Access Control System for the University.

The Contractor is required to use the Standards as the foundation for the system design. However, the site specific operational, logistical and performance requirements of the respective project shall be observed.

The Contractor shall provide Macquarie University with a complete cost-effective installation of finished works thoroughly tested and ready for operation.

The designed solution shall provide additional Electronic Security and Access Control coverage at the nominated locations throughout the University and associated facilities.

The works to be carried out shall include, however not be limited to the following:

- i. Supply, install, program and commission the additional infrastructure requirements for the ISMS;
- ii. Supply and installation of non-proprietary hardware including, however not limited to Electronic Locking solutions, Readers, Controllers, Cables, Power Supply and peripheral equipment to comply with this Specification;
- iii. Install, set up and configure the integrated ISMS (Gallagher) and all associated peripheral equipment;
- iv. Supply and install all site structured cabling infrastructure, including cable supports, conduits, junction boxes, access and penetrations required to accommodate the integrated solution;
- v. Include all subsequent trenching and additional infrastructure required to provide a turnkey solution.

2.2 Performance Objectives

Contractors are to allow for a professionally installed and fully operational system such that Macquarie University can achieve the maximum advantage from the operation of the solution and equipment, providing a beneficial system which is reliable, functional, and simple in its operation.

The minimum requirements for the installation of the Access Control and Electronic Security equipment are to:

- i. Provide adequate and suitably controlled access and alarm monitoring coverage to nominated areas;

- ii. Meet all equipment and operational requirements as specified;
- iii. Comply with all state statutory and regulatory provisions with particular emphasis on the Occupational Health and Safety BCA and Disability Discrimination Act (DDA) and Security Licensing Acts and Regulation, and;
- iv. Be Fit for Purpose and designed to provide a complete, functional and operational solution with minimal lifecycle costs.

2.3 Standards

The installation shall be in complete accordance with the current editions of all applicable standards. The following standards although not exhaustive provide the basis for compliance, it shall be the Contractor's responsibility to ensure all equipment and works supplied and carried out meet and comply with the relevant Local, State and National standards.

AS 3000: Electrical Installations (Wiring Rules)

AS 3008: Electrical Installations – Selection of Cables

AS/NZ S3010: Electrical Installations – General Sets

AS 3439: Low Voltage Switchgear and Control Gear Assemblies

AS/NZS 61439: Low Voltage Switchgear and Control Gear Assemblies

AS/NZS 4251: Electromagnetic Compatibility (EMC) – Generic Emission Standard

AS/NZS CISPA.14.1 2.3.1 Equipment Radio Frequency Interference

AS4145.2.2008 SL8 (Security) Australian Lock Standard

AS4145.2.2008 D8 (Durability) Australian Lock Standard

AS1905.1. 2005 fire rated up to 4hrs on fire door assemblies

CE Approved

C-Tick Certified

3 Design Parameters

The works to be carried out shall comply with, however not be limited to the following:

- i. All equipment to be provided must be new (unless noted and accepted otherwise) and must be capable of performing its function as intended by the Specification;
- ii. All equipment to be supplied must be of proven quality from well-known and established manufacturers and local established distributors with local spares and engineering support readily available;
- iii. All cables installed on building externals or cables installed in accessible locations i.e. where MQU considers the cables to be accessible (to be determined by the MQU's Authorised Representative);
- iv. All external ducting/conduit under 3000 mm and all internal ducting/conduit must be steel and vandal proof. All ducting/conduit must be pre-approved by the MQU's Authorised Representative prior to installation;

- v. Existing conduits may be reused at the Contractor's risk during the twelve (12) months Defects Liability Period (DLP). Any re-used equipment will be treated as new for the purpose of the DLP;
- vi. Any unused conduits in risers shall not be removed but capped and labelled;
- vii. All penetrations seals are to be maintained for fire and acoustic integrity and make good to existing surfaces where unused equipment has been removed;
- viii. (As required) Supply and installation of all final power sub-circuits and backup UPS power supplies;
- ix. (As required) Supply of all cabinets, racks and associated fittings.

3.1 Other Requirements

- i. Lead times for replacement parts must be no longer than two (2) weeks;
- ii. Contractors may be requested to validate their initial design through demonstrations;
- iii. The Contractor must provide all plant, materials, equipment, services and personnel necessary to carry out the works and the maintenance under the Contract;
- iv. The provision of all derived power circuits and power supplies must form part of the works (all 240v outlets by the Contractor shall be provisioned using licenced Electricians to Australian Standards).

3.1.1 Equipment Radio Frequency Interference

Equipment shall comply with the requirements of AS/NZS CISPA.14.1 with regard to the generation of radio frequency interference. If required, suppression devices or shielding devices shall be installed.

3.1.2 Equipment Electromagnetic Compatibility

Equipment shall comply with the requirements of AS/NZS 4251 with regard to the generation of electromagnetic emissions.

3.1.3 Energy Conservation

Low energy, high efficiency equipment shall be incorporated in all University projects. The design for the ISMS shall be in accordance with the requirements of the National Construction Code for Energy Efficient Installations.

3.1.4 Life Cycle Costs

Equipment selection and system design shall ensure the most effective life cycle costs by minimising maintenance costs and taking into consideration the expected life of the equipment.

3.1.5 Expansion

The proposed solution shall be designed to allow for easy expansion at any time without requiring radical changes or reconfiguration. The contractor shall allow for the capacity to provision 10% additional system and supporting infrastructure to allow for future system expansion.

4 Alternate Equipment

Macquarie University acknowledge that new products, equipment models and solutions are continually changing, therefore the following specifications are the preferred “benchmark” of the minimum requirements.

Alternatives may be proposed and submitted by the contractor for consideration. Any alternatives submitted must be supplied with supporting documentation outlining where the proposed alternative exceeds the performance benchmark and provides Macquarie University with a leading-edge solution.

- i. Alternatives will only be considered when accompanied by a compliant solution utilising the performance benchmarks outlined;
- ii. No alternative equipment or solution shall be installed on any particular site, unless permission is authorized by MQU’s Authorised representative, with the alternative solutions or products specifically accepted for use on the site;
- iii. Acceptance of an alternate product or solution on one of the University buildings does not automatically provide acknowledgement or acceptance on other sites within the existing campus; as such permission should be sought by the contract or prior to proceeding with any alternate product or solution on each occasion.

5 Project Obligations

Prior to the commencement of any works the Contractor must submit to the Authorised Representative, full design documentation and Shop Drawings outlining what is to be provided for the works and the phasing of the Works Program, including, but not limited to the following:

- i. A list of all personnel involved with the contract, including licensing details;
- ii. Copies of current Certifications held by all personnel;
- iii. Evidence that the Contractor is an authorised Channel Partner of Gallagher;
- iv. A work program, methodology statement and implementation plan for each phase and solution;
- v. Completed Safe Work Method Statement (SWMS) identifying hazards and systems controls in place per site;
- vi. Equipment schedules showing device type, make, model and quantities;
- vii. Samples of all equipment (upon request);
- viii. Equipment installation manuals;
- ix. Equipment programming manuals and schedules;
- x. Equipment interconnection details, site layout and system block diagrams (including equipment locations, cable routes and identifiers) and cable schedules including cable type, description and identifier.

5.1 ‘As Installed’ Drawings

On completion of the works, prior to the issuing of the Practical Completion Certificate, the Contractor shall provide a complete set of drawings showing all the services ‘as-installed’ on site.

The drawings shall be to scale as the design drawings and shall record details of the installed works.

The drawings shall include a clear and precise symbols and description legend depicting all items supplied marked as "as installed" drawings.

The location information shown on the drawings shall be accurately represented, measured from permanent building boundaries or other permanent features.

The drawings shall be provided on electronic media in both PDF format and DWG format.

5.2 Operational and Maintenance Manuals

One (1) hard copy of Operating and Maintenance Manuals shall be provided by the Contractor in the following format together with one copy provided in PDF format on electronic storage media. All Manuals shall be customised as per MQU's O&M template.

As a Minimum the Contactor shall provide the following;

- i. A4 size loose-leaf sheets bounded with hard covers suitable for easy reference and mid to long term storage;
- ii. Each binder shall be indexed, divided into system elements and titled.
- iii. Binders shall include a typed or printed title on both the cover and the spine to clearly identify, showing the project name, location and relevant section numbers.

5.3 Template

The format and contents of the manuals shall follow the following format:

General Description of Project

- i. System operation
- ii. Design parameters

Operating Procedures

- i. General
- ii. Automatic/Manual operation
- iii. Routine inspection and reporting templates
- iv. Fault finding information

Maintenance procedures

- i. Maintenance procedures for plant & equipment
- ii. Manufacturers recommendation
- iii. Templates and matrix tasks for all items applicable to AS 1851

Maintenance schedules

- i. Plant and equipment schedules
- ii. Spare parts list
- iii. Manufacturers contact details

Manufacturers literature & warranties

- i. Commissioning documentation
- ii. Data specification sheets
- iii. Manuals
- iv. Certificate of Compliance
- v. Asset register (excel format) with hyperlinks to the sections listed above, Drawings in PDF and DWG

6 Compliance and Statement

6.1 General

Any items of equipment or performance standard proposed to be supplied by the Contractor, which deviates in any manner from the specified requirements, shall be declared as a variation.

For all items of equipment, installation method/s or sequencing not declared in this statement, the specified requirements shall be deemed to be offered by the Contractor, without qualifications, and all associated costs shall be deemed to be included in the tender price.

Any variation requires written authority from MQU's Authorised representative prior to the acceptance of alternative equipment and / or installation variation.

6.2 Statement

The Contractor shall as part of the proposal, include a complete compliance statement to support their offer. The Compliance Statement shall consist of a statement for every section and clause within this document, that states either the following;

- i. **Complies** – Meaning the Contractors offer completely complies to all aspects of the section, product or Clause;
- ii. **Non-Complies** - Meaning the Contractors offer does not comply to the section, product or Clause;
- iii. **Partially Complies** - Meaning the Contractors offer partially complies to the section, product or Clause. (Note; all sections that partially comply, must be supported by and explanation that state the reasons, or areas of non-compliance);

Also note: The Compliance Statement will be included as part of the weighting, and any proposals submitted without a comprehensive compliance statement will be scored as such and may be disallowed as part of the review process.

7 Glossary

Term	Definition
ACA	Australian Communication Authority
AS	Australian Standard
AMT	Alarms Management Terminal
ACM	Asbestos Containing Material
BCS	Building Code of Australia
BGU	Emergency Break Glass Switch (Door Release / Fire / Duress)
DDA	Disability Discrimination Act
DOTL	Door Open Too Long Alarm
DWG	AUTO CAD Drawing Package
DNL	Door Not Locked Alarm
DPDT	Double Pole Double Throw Contact
DLP	Defects and Liability Period
ELD	Encrypted End of Line Device
ESF	Energised Security Controller
ELM	End of Line Module or Resistor to monitor a short circuit or breach of the circuit.
IFC	Intelligent Field Controller
ISMS	Integrated Security Management Solution, Electronic Security and Access Control
IP66	"Ingress Protection": ratings are defined in international standard EN 60529 used to define levels of sealing effectiveness
PIR	Passive Infrared Detector
SMS	Security Management System
GUI	Graphical User Interface
LSS	Lock Status Sensor
MQU	Macquarie University
REX	Request to Exit
LAN	Local area network
MQU IT	Information Technology Directorate: The MQU department responsible for the delivery and operations of information technology and related services.
OVP	Operating Viewing Platform (CCTV Workstation)
SWMS	Safe Work Method Statement
PDF	Open Source Document
DSS	Door Status Sensor by Reed-Switch
System	All of the components that go together to produce a working entity including hardware, software, communications infrastructure, processes and protocols.
Server	A computer platform established primary for the purpose of storing digital video files intended to be used by other workstations across a computer network
Must, will, shall	The statement is mandatory
Should	The statement is advisory
System	All of the components that go together to produce a working entity including hardware, software, communications infrastructure, processes and protocols.
Authorised Person or representative.	Person or authority designated by MQU to adjudicate and/or make decisions on behalf of MQU

8 Technical Requirements

8.1 Door Hardware

The following provides an established set of minimum requirements and standards for Access Control and Electronic Security for the University. They are based on previous experience utilizing established technology that provides installation and operational efficiencies, including the reduction of false alarms.

As a minimum requirement all doors fitted with Access Control and Security locksets shall include, however not be limited to the following functionality;

- i. DOTL - Door Open Too Long Alarm;
- ii. DNL - Door Not Locked Alarm;
- iii. Fire Trip – 24VDC Activation;
- iv. Fail Safe – Power on to Lock;
- v. Fail Secure – Power on to Unlock;
- vi. Forced Door Alarm;
- vii. RTE – Request to Exit;
- viii. Door Positioning Monitoring;
- ix. 1000kg Holding Force;

8.1.1 Electronic Mortice Lock

Integrated Electronic Mortice Lock set options is acknowledged and accepted for perimeter door applications, where the door thickness is between 32-50mm. All cable transfers to conceal wiring on the hinged side of the door are to be concealed within the door. Note; surface mount cable transfers will not be accepted.

As a minimum Electronic Lock Sets shall include however not be limited to the following;

- i. Continuously rated to operate on 12Vdc - 24Vdc Operating Voltage;
- ii. 500mA (max), 80mA holding @ 12Vdc;
- iii. 275mA (max), 50mA holding @ 24Vdc;
- iv. Dual Key override Monitoring;
- v. Deadlatched Monitoring;
- vi. Locked Monitoring;
- vii. Door closed Monitoring;
- viii. Request to exit;
- ix. Microswitches: 500mA (max) @ 30Vdc each circuit;
- x. Reed switch: 100mA (max) @ 30Vdc;
- xi. Operational temperature range -20c to + 60c;
- xii. Back set - 60mm standard, 89 & 127 mm available;
- xiii. Latch Bolts - Reversible with Stainless Steel construction;

- xiv. Door Clearance 3 - 6.5 mm;
- xv. Cylinder Standard Lockwood oval shaped cylinders;
- xvi. Cabling - 1.6 metre length of cable with 12 pin socket 18AWG (0.82mm²) cable runs up to 30m.

In addition, monitored locks must be capable of monitoring the following functions: Key override, door position / reed switch, selectable hub / Request to exit, & locking bar status. All monitoring outputs must have the ability to be wired independently. All settings – including fail safe / fail secure, handing, hub selection must be field configurable.

Mortice Lock sets shall be installed with the appropriate Rebate Kits with extended cylinders on doors that exceed 50mm in thickness.

8.1.2 Electronic Door Strike

An electronic Door Strike used in conjunction with an approved Mortice Lock set or Face Plates that provides door position monitoring is acceptable for perimeter and internal door applications.

The strike shall include an integrated reed switch that when combined with an approved specialised Mortice lock and tongue sensor, provides active door position monitoring.

For half leaf and double doors, all cable transfers to conceal wiring on the hinged side of the door are to be concealed within the door, surface mount cable transfers will not be accepted.

As a minimum, Electronic Door Strikes and approved Lock Sets shall include however not be limited to the following;

- i. Field selectable fail safe/fail secure;
- ii. Multi voltage 10-30Vdc;
- iii. Fully monitored - Integrated door position (reed) switch - Solenoid/Locked - Latch position;
- iv. 1000kg holding force;
- v. 4hr fire rating;
- vi. Mounting tabs as supplied standard;
- vii. Weather Resistant (IP54);
- viii. Built in Protection Diode.

In addition, the Door Strike shall be constructed of stainless steel with a minimum holding force of 1000kg and an endurance rating of 1.5 million cycles. Monitoring must include independent latch and solenoid monitoring. The strike shall have an integrated reed switch for door position monitoring and used in conjunction with the approved Mortice lock set or face plate.

8.1.3 Pre-load Pressurized Doors (Harsh Environments)

Pre-load is a common condition that is caused by differential air pressure created when heating and cooling systems are in use, or the weight of warped or drooping doors applies pressure on the Strike mechanisms, requiring the user to pull on a door before it unlocks.

In addition to the minimum standards and requirements stipulated for Electronic Door Strikes, the Contractor shall ensure that in harsh applications where air-conditioning or variations in air pressure, create an operational load on the door, Electronic Door Strikes that remain operational under a pre-load pressure of up to 25kg shall be provisioned.

8.1.4 Electromagnetic Locks

All single and double Electro Magnetic Locks shall as a minimum have a holding force of up to 280kg, and Fire tested up to a 4-hour fire resistance rating tested to both Australian and British Fire Test Standards. The device shall include built in surge protection and accept both 12 and 24VDC. The Electro Magnetic Lock shall also provide an external long-distance visibility Light Panel (LP) and the following monitoring features.

- i. Lock Status Sensor by Hall-Effect (LSS);
- ii. Door Status Sensor by Reed-Switch (DSS);

The Electro Magnetic Lock must be of proven quality and supplied with an Anti-Tamper-Plate as standard, to prevent hostile attacks on the dome-nut-fixing bolt of the Armature Plate.

As a minimum, Electro Magnetic Locks shall include however not be limited to the following;

- i. Door and Lock Status Monitoring Sensor;
- ii. Built-in varistor (MOV) surge protection;
- iii. Light Panel for long distance visibility;
- iv. Satin anodised aluminium housing and zinc plated electromagnetic lock body;
- v. Carbon free steel armature plate;
- vi. Guaranteed no residual magnetism;
- vii. CE & C-Tick;
- viii. 4-hour fire tested;
- ix. Anti-tamper Plate.

8.1.5 Integrated Wireless Mechanisms

Non-essential doors, such as internal back-of-house offices and low usage doors shall be provisioned with a purpose-built unified wireless Lock Sets, that support inbuilt Access Control Reader, (PIN) Code Pad and Electronically Motorised Door release mechanisms. The nominated doors fitted with these locksets shall provide full functionality of door operation from a self-contained wireless operated solution.

The doors requiring integrated wireless locking mechanisms as shown on the design Brief documentation and drawings shall include, however not be limited to the following:

- i. Embedded wirelessly activated locking mechanisms;
- ii. Request to exit internal lever monitoring;
- iii. Built-in RFID card reader;
- iv. Wireless online access control;
- v. Audit trails in time zone management;
- vi. Additional key override;
- vii. Door position switch;
- viii. Inbuilt off-line credential Cache for the last 200 users;
- ix. Battery powered for up to 40,000 operations;

- x. LED status;
- xi. Low battery warning alarm;
- xii. Support multiple RFID credentials and Seos mobile access;
- xiii. Programmable Handshake communication from 5 – 10 seconds;
- xiv. Keypad operation via 12 Character keypad;
- xv. Support audit trails and time zone management;
- xvi. Support contacts closures for emergency Break Glass override;
- xvii. Fully integrate with the Universities Access Control Solution.

8.1.5.1 Integrated Door Lock Functionally,

External activation - The door lock shall be set so that the external lever is always locked requiring the presentation of a valid swipe card to enable the activation of the lever. The door lock shall automatically relock after a set time period, however, has the ability to be activated via the built-in touch keypad or key override.

The wireless integrated door lock shall have the ability to be programmed from the Integrated Security Management Solution (ISMS) for timed access where the lock will remain in the unlocked state during normal operating hours, and automatically switch to the lock state outside of the programmable operation hours, requiring the use of a valid swipe card to grant access.

Internal Activation - The internal lever is set to activate free egress at all times, the system allows for the ISMS to recognise a valid egress from the activation of the internal lever for fail safe secure but safe operation.

Door monitoring - The solution shall include door monitoring to detect forced entry and communicate to the ISMS forced entry and door open too long alarms.

Fail secure, Fail safe - integrated door locking systems shall provide fail secure and fail safe operational modes. From the keylock side of the door the functional requirements of the lock shall operate upon the presence or removal of power, shall be as follows:

- i. **Fail Secure** – This mode stipulates that the door is locked from the outside when power is removed.
- ii. **Fail Safe** - This mode stipulates that the door is unlocked from the outside when power is Removed.

It is a requirement that the set-ups of all Fail Secure doors provide free internal egress at all times unless stipulated, and/or are fitted with additional emergency failsafe release mechanisms in accordance with BCA regulations.

A single, seamless user interface shall be provided within the head end to ensure integrity of access decisions are maintained within the primary access control system. The flow of information from the RFID card shall be transmitted instantaneously to the wireless card reader/lock, which shall in turn send the card credentials to the hub and access control system.

The primary Access Control and Intruder Alarm system shall provide real-time access privileges for both online wired and wireless doors through a single interface. Card encoding shall be carried out as a single encode operation for both wired and wireless door readers.

8.1.6 Integrated Door Wireless Communication Hub

Integrated door locks shall operate over an encrypted 2.4 GHz wireless link to communication hubs throughout the facility. The communication HUBs shall act as the link between the integrated door locks and the Unified ISMS solution.

The Wireless communication hubs shall as a minimum support the following:

- i. Communicate to each lock set over a 2.4 GHz encrypted wireless network;
- ii. 128 Bit AES Encrypted Radio Communications;
- iii. Integrated antenna;
- iv. Led Status for visual indication;
- v. Control a minimum of eight integrated lock sets;
- vi. Communicate to the ISMS via Weigan, Advance Weigan, RS-485 or IP (Ethernet);
- vii. Minimum operating transmission distance of 25 m.

The wireless RS485 communication hub shall support up to 8 wireless integrated door locks or cylinders and have reliable communication to each reader within a distance of 15 metres.

Wireless hubs shall have the ability to be wired in series with RS485 compatible cable.

The wireless hub shall conform to the radio standard applicable to the region of installation and conform to IEEE802.15.4 (2400 – 2483.5 MHz).

AES 128bit encryption shall apply for communication between the hub and each wireless reader.

Up to 16 (installer selectable) channels per hub shall be available to ensure each wireless integrated door lock or cylinder is configured with reliable communication.

8.1.7 Movement Detectors

Areas that are not operational 24 Hours shall have Passive Infrared Movement Detectors (PIRs) specified. PIRs provide movement detection within armed areas. PIRs work in conjunction with door open status (reed switch) monitoring to provide after-hours security to non-operational areas.

The Contractor shall provide an industry standard dual technology with quad zone logic lens, aspherical lens detector with sealed optics designed to provide wide angle coverage for rooms and open spaces, and interchangeable or models that provide narrow beam direct coverage for hallways etc.

These passive infrared movement detectors shall be end of line monitored, and upon activation shall alert security and any off-site monitoring facilities via the Access Control and Security Solution, of the time of the event and location within the facility.

PIR Movement Sensors shall as a minimum have, however not be limited to the following;

- i. Dual technology (PIR/Microwave), and;
- ii. Detector cover tamper switch to be connected to the Access Control / Security Solution;
- iii. Anti-Masking.

It shall be the Contractor's responsibility to select, set up and position the detectors for the most stable response, taking into account heaters, fans and any other adverse environmental conditions.

8.1.8 Reed Switches

All doors excluding integrated lock set mechanisms, shall be supplied with complying industry standard concealed or approved surface mount reed switches that are suitable for each door type and location.

These reed switch devices shall be end of line monitored, and upon activation shall alert security and any off-site monitoring facilities via the ISMS of the time of the event and location within the facility or trigger an alarm in the event of a door being forced open or left open too long (DOTL).

8.1.8.1 Doors

Flush magnetic reed switches shall comply with the following:

Be installed on nominated internal and perimeter doors as indicated on the drawings:

- i. Bench Marked, Sentrol 1078 series type or approved equivalent;
- ii. On the top of the door 100 mm from the leading edge, and;
- iii. Positioned on the opposite side of hinge or pivot.

In cases where concealed Reed Switches are not practical due to door construction or other reasons, the Contractor shall submit suitable supporting documentation and samples for approval. E.G. Mortice Locks with DOTL installed on the frame.

8.1.8.2 Roller Shutters

Surface Mount heavy duty Roller Shutter reed switches shall comply with the following:

- i. Be installed on roller doors, gates as indicated on the drawings;
- ii. Have no exposed cable;
- iii. Positioned so as not to be damaged by vehicles, other traffic, and;
- iv. Corrosion resistant/weatherproof where required;
- v. Bench Marked, Sentrol 2202A series type or approved equivalent.

8.1.9 Request to Exit (REX) Button

All doors without free handle egress such as automatic doors or doors fitted with Mag locks as shown on the design drawing shall be fitted with an approved REX Button. This button shall operate and override the locking mechanism allowing egress.

The Green Request to Exit button shall be installed as stipulated as per the design drawings. As a minimum the REX devices shall include, however not be limited to the following:

- i. Mushroom Button shall be Green in Colour;
- ii. Be mounted on a stainless-steel wall mounted plate;
- iii. Be engraved in readable letters readable from a distance of 3 metres 'PRESS TO EXIT';
- iv. Contacts shall be Double pole double throw Type of actuation;
- v. Activation shall be spring loaded Momentary;

- vi. Max. Ratings: 5A@250 Vac, 6A@24V DC;
- vii. Operating travel: 3.2 mm;
- viii. Operating temp. Range: -20~+70C Contact resistance: 50 mΩ;
- ix. Operating life: Over Mechanical 100,000 times.

REX Buttons must be mounted visibly 500mm away from the leading edge of the door or from the corner (hallways) as per DDA requirements. Installation height of the REX device shall be 1000 mm ±200 mm, measured from the middle of the Button to the floor unless otherwise stipulated.

All REX Buttons must be adequately illuminated by natural light or other light source (including emergency lighting if present).

It shall be the Contractors responsibility to ensure all building regulations and certifications including BCA and DDA are observed and adhered.

8.1.10 Duress Alarms

Duress buttons shall be connected to the ISMS alarm inputs and programmed to be active as a 24-hour device. Each duress alarm signal must Register on the MQU Security Control Room workstations and any remote security monitoring location, as a high priority alarm and sound an audible tone at the Workstation to attract attention.

Duress buttons / switches shall be installed in areas as stipulated with the Design Brief documentations or site drawings. The final position of the devices is subject to approval by MQU's authorised representative.

The push-button must be selected and installed such as to prevent accidental activation. When activated, the device must latch until manually reset on the switch at the location.

8.1.11 Desk Mounted Duress Switch

An approved Slider type dual button push buttons with key reset shall be installed under counters and desks as stipulated or described in the documents.

The Contractor shall Locate push buttons at counters and desks positioned so that they may be depressed by persons seated at the desk or standing at a counter. Where desks contain drawer units, the Contractor shall fix the duress button to the side of the unit, 25 mm below the desktop draw. Locate all switches a fixed distance (nominal 25 mm) back from the edge.

8.1.12 Wall Mounted Duress Switch (Heavy Duty)

As stipulated in the Design Brief and supporting drawings, the Contractor shall provide and install a complying Wall type duress push button. The Switch shall as a minimum provide, however not be limited to the following:

- i. Mushroom heads with twist to reset;
- ii. The push buttons shall be coloured Red and must be engraved 'EMERGENCY';
- iii. Mounted at a height of 700, 1000 and or 1500mm as stipulated;
- iv. Be Double Pole Double Throw DPDT.

Prior to installation, the Contractor shall provide specification data sheets, and if requested samples of the proposed device for approval by MQU's authorised representative.

8.1.13 Call Point Emergency Break Glass Unit (BGU).

All emergency manual Glass Break Call Point Switches shall be manually activated by depressing the black mark indicator that breaks the units glass pane thus triggering the switch that activates the alarm.

The Alarm activation shall trigger an LED display on the front of the unit to indicate that the alarm has been activated. Resetting this alarm shall be achieved with the replacement of the glass panel and / or reset key that automatically resets the unit's LED indicator light.

The approved BGU shall as standard have the ability to activate and reset the unit with a test key for testing purposes.

BGU shall be available for the following applications:

- i. Emergency Fire. (Colour RED);
- ii. Emergency Door Release. (Colour GREEN);
- iii. Emergency Duress. (Colour White).

BGU shall be suitable for both indoor and outdoor applications with a minimum protection category of IP54 of indoor and IP66 for external applications, be of durable construction, vandal resistant. All BGU shall as a minimum provide, however not be limited to the following:

- iv. Double Pole Double Throw DPDT;
- v. Ability to be activated and reset via a Test Key;
- vi. PVC Coated Glass Element;
- vii. Readily available replacement Glass Panels;
- viii. Indicator LED for alarm or for inspection evaluation;
- ix. Available in Surface or Recessed Mount.

BGU must be mounted visibly along escape and rescue routes (e.g. exits, passageways, stairwells) and be easily accessible. Installation height of 1000 mm \pm 200 mm, measured from the middle of the manual call point to the floor unless otherwise stipulated must be maintained.

All BGU must be adequately illuminated by natural light or other light source (including emergency lighting if present).

It shall be the Contractors responsibility to ensure all building regulations and certifications including BCA and local Fire services are observed and adhered.

Fire Trip: Power to all BGUs for fire trip and door activation and ancillary devices shall be 24VDC.

8.1.14 Card Readers.

All card readers shall be Gallagher T-Series that utilise RS485 HBUS protocol with a response time of 200 Milliseconds. The readers shall have the ability to support multiple card technologies including MIFARE.

All readers shall be IP68 environmental protection and IK07 for impact protection, Contemporary design - classic black and white, with flush mounting variants with configurable illumination and sound.

The Access Control Card Readers shall as a minimum provide and support the following:

- i. Mifare Classic;
- ii. Mifare Plus;
- iii. Mifare DESFire EV1;
- iv. Near Field Communication (NFC).

The reader shall be capable of reading the card serial number (CSN) of the Mifare cards. The readers shall support self-discovery on MQU's ISMS.

All Readers shall contain a unique serial number. When connected to an Intelligent Field Controller (IFC), the serial number of the reader shall be reported to The System. Once assigned to a function within an IFC, any attempt to substitute readers in the field without authorisation shall instigate an alarm within the solution.

Data communication rate between IFCs and readers shall be at least 1Mbit/second. Communication sessions between IFCs and readers shall use certificate exchange protocols using keys with a minimum strength of 256-bit elliptical encryption.

Data communication between IFCs and readers shall use a minimum of 128-bit AES encryption.

Readers shall generate a heartbeat signal to enable the IFC to identify lost communications and thereby generate an alarm.

Readers shall be upgradeable via software downloaded from The System without any intervention at the reader.

The reader shall accept messages from the IFC to advise that data from reader to IFC has been received, the receipt of a successful communication shall halt the transmission of the card data.

Each reader shall be identified independently on the System by means of a unique plain language descriptor. The plain language descriptor shall be at least 60 characters in length.

Where a card only reader is specified, the reader shall include an audible sounder and red/green LEDs to provide user feedback. The sounder shall give different beeps to indicate the following:

- i. Access granted;
- ii. Access denied.

Furthermore, Readers shall provide the following:

- i. A steady red LED shall indicate door secure;
- ii. A flashing red LED shall indicate access denied;
- iii. A steady green LED shall indicate door free access;
- iv. A flashing green LED shall indicate access granted;
- v. It shall be possible to turn off the reader LED indication via The System software;
- vi. It shall be possible to turn off the reader beeper via The System software;
- vii. Readers must comply with at least IP68 environmental protection rating;
- viii. Readers must comply with an impact rating of at least IK07.

A vandal resistant enclosure having an impact rating of at least IK08 rating shall be provided where:

- i. Vandal covers shall be fixed to the wall surface using tamper-resistant screws;
- ii. Vandal covers shall have bevelled edges to limit the ability for persons use the reader as an aid to climb or gain a foothold;
- iii. All external surfaces shall be bevelled and without protruding parts to meet anti-ligature requirements;
- iv. All readers must be RoHS compliant;
- v. Reader shall operate with a temperature range of -30oc to +70oc.

8.1.15 Pin Card Readers

Where a card reader with PIN pad and display is stipulated in the design brief and drawings, the reader shall include:

- i. A minimum of a 3.5" LED colour display;
- ii. Backlit keys;
- iii. The reader shall display information to the user using a combination of text and graphics;
- iv. The reader shall display the date and time.

All readers shall be capable of (but not limited to) carrying out the following functions:

- i. Arm and Disarm alarm zones. A minimum of 50 per reader must be supported;
- ii. View Alarms. A minimum of 100 per reader must be supported;
- iii. Acknowledge alarms. A minimum of 100 per reader must be supported;
- iv. View alarm history. A minimum of 100 per reader must be supported;
- v. Change the door to Free and Secure Access mode;
- vi. Change the door to operate from a user defined schedule;
- vii. Turn outputs on and off. A minimum of 50 per reader must be supported;
- viii. View the status and Isolate inputs. A minimum of 100 per reader must be supported;
- ix. Tamper protection shall be provided against the unit being removed from the mounting surface;
- x. Readers shall operate with a temperature range of -30c to +70c and comply with an impact rating of at least IK07.

8.1.16 Intelligent Field (Door) Controller (IFC)

The Intelligent Field Door Controllers shall be Gallagher 6000 series IP Based units, capable of managing all localised access control, intruder alarms, perimeter security and automation. The Controllers shall be capable of operating independently from the Command Centre server.

The controller shall have the ability to support multiple field devices such as T Series Readers and T20 Terminals, Door Modules, I/O boards, End of Line Modules (ELM) via the

HBUS RS485 controller, and additional 4 or 8 channel modules via H series expander modules.

At each field location the controller shall communicate with the Gallagher Command Centre via an Ethernet connection, and the Contractor shall provide all the necessary cabling, connection and field equipment to the pre-determined designated interface point provided by MQU's IT department. The Contractor as part of their works shall liaise with MQU's nominated representative confirming the design and required infrastructure to provide the necessary connections and provisioning for a fully functional complete set of works fully tested and ready for operation.

As a minimum each door controller shall provide, however not be limited to the following:

- i. IP based 10/100 Ethernet connectivity, with 1Gb network;
- ii. Access control support for up to 10 wired doors, with multiple readers configurable per door;
- iii. The ability for intruder alarms monitoring and transmission to external monitoring stations;
- iv. Programmable controller-based logic, able to operate independently of the server;
- v. Support for elevator access control;
- vi. Provide encryption between the controller and readers;
- vii. Support for multiple wiring topologies, for existing field devices;
- viii. Peer-to-peer inter-controller monitoring;
- ix. Provide support for 256 alarm zones, 2000 access groups, 500,000 card holders, and 80,000 events;
- x. Support High Level interface with Aperio;
- xi. T-Series HBUS, CardaxIV, and 3rd party Wiegand, and OSDP;
- xii. 8H / 4H Module – Connecting directly into the controller, supporting respectively 8 or 4 readers and door I/O (HBUS);
- xiii. The controller shall support advanced access control functions such as mobile credential support, anti-passback, anti-tailgating dual authorization, elevator floor access, and visitor escorting functions;
- xiv. Used in conjunction with the Gallagher T20 Terminal, the C6000 supports full intruder alarms functionality, including arming and disarming, entry and exit paths, sensor walk testing, and high security options such as authenticated and encrypted sensor communications and sensor masking detection alarms.

8.1.16.1 IFC Hardware Function

The Intelligent Field Controller (IFC) shall be the main controller in the field. The Security Management System shall communicate directly with all IFCs. Each IFC shall be intelligent such that in the event of failure of power or communications to The System, for whatever reason, the system shall continue to allow or deny access based on full security criteria.

The IFC shall store on-board all the security and access parameters to operate completely independently from the central control server and shall buffer activity data and immediately transmit it to the central control server upon reestablishment of communications. Should communications fail, each IFC shall be capable of buffering up to 80,000 events.

As a minimum the Intelligent Field (Door) Controller (IFC) shall provide however not be limited to the following:

- i. All events shall be time-stamped at the IFC at the time of occurrence;
- ii. The IFC shall be capable of storing up to 500,000 card records with associated access criteria;
- iii. The system shall monitor input circuits and enunciate whether the circuit is Normal, Alarm, Open Circuit Tampered or Short Circuit Tampered as separate conditions;
- iv. A configurable range of ELM end of line resistor values shall be supported as a software function to support pre-existing input circuits when required;
- v. The IFC shall include tamper protection for the front and the back of the panel. The front panel shall be tamper protected for door open, and the rear of the panel to detect if the panel has been removed from the wall. These shall use optical tamper detection. Mechanical tamper devices are not acceptable;
- vi. The IFC shall incorporate an ARM 9 processor with at least 256 Megabytes of non-volatile FLASH EEPROM. The IFC shall incorporate boot code in a protected sector of the flash memory. For software upgrades, all system software shall be downloaded from the central server over the network;
- vii. The IFC shall support direct download via USB to allow local upgrades;
- viii. The upgrade process shall only accept authenticated downloads via the USB port;
- ix. The IFC shall operate from a separate battery backed 13.6V DC supply;
- x. The system shall be capable of automatically detecting and reporting a power failure low battery and battery not connected;
- xi. IFCs shall automatically restart and resume processing following a power failure;
- xii. IFCs shall be fitted with 'watchdog' hardware and software to provide automatic detection and restart should the processor lock up;
- xiii. The IFC shall contain its own real time clock. The clock shall be synchronised with the central control server clock at least once per hour. The accuracy shall be such that the time difference between IFCs shall not vary more than 0.5 second at any time;
- xiv. The IFC shall have an on-board Ethernet (TCP/IP) connection and driver supporting 10BaseT and 100BaseT operation;
- xv. When specified, the IFC shall support 100/1000BaseT;
- xvi. The IFC shall have the ability to be fitted with 2 Ethernet ports providing an alternate communication capability;
- xvii. The System and Intelligent Field Controllers shall have IPv6 address support;
- xviii. The IFC shall be provided with a pre-configured IP address to allow off-line initial configuration via a web browser application when required;
- xix. The IFC shall support DNS (Domain Name Server) operation;
- xx. Should the primary DNS not be available, the IFC shall be able to automatically establish contact with a secondary or tertiary DNS;

- xxi. Should excessive network broadcast traffic occur (resulting from a denial of service attack or similar), an alarm shall be generated;
- xxii. All data communication between The System and IFCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 256-bit AES or stronger;
- xxiii. Communication between The System and IFCs shall be on-line and monitored for interruption;
- xxiv. The IFC shall include one RS 232 multi-communications port;
- xxv. The IFC shall include one USB 2.0 port;
- xxvi. It shall be possible to view the IFC status and configuration for commissioning and diagnostic purposes without the use of the central server software or other proprietary software. This may be achieved by the use of a conventional web browser. In high security applications, it must be possible to disable this feature at the IFC;
- xxvii. The IFC Logic Block output shall be able to trigger actions across multiple IFCs, independent of The System being online;
- xxviii. A separate alarm message shall be transmitted to The System for at least the following alarm conditions. The alarm message shall be displayed in plain language text:
 - xxix. Tamper;
 - xxx. Tamper Return to Normal;
 - xxxi. Unit Stopped Responding;
 - xxxii. Card error;
 - xxxiii. Maintenance Warning;
 - xxxiv. Alarm Sector State Change;
 - xxxv. User Set;
 - xxxvi. User Unset;
 - xxxvii. Card Trace;
 - xxxviii. Wrong PIN;
 - xxxix. Access Denied;
 - xl. Duress;
 - xli. Zone Count Maximum;
 - xl.ii. Zone Count Minimum;
 - xl.iii. Door Open Too Long;
 - xl. iv. Forced Door;
 - xl. v. Door Not locked;
 - xl. vi. Power Failure;
 - xl. vii. System Reboot;

- xlvi. Intercom.
- xlix. The IFCs shall communicate with and control the following equipment:
 - a. Biometric access readers;
 - I. Card access readers with PIN keypads;
 - ii. Elevator access equipment;
 - iii. Alarm monitoring Input/output panels and equipment;
 - liii. Alarm response equipment.
 - liv. Any failure of a biometric reader unit and its communications with the IFC shall be raised immediately as a high priority alarm and shall not cause the IFC or other associated hardware to stop working correctly;
 - lv. The IFC shall communicate with remote devices (biometric readers, alarm equipment, elevator readers) using a fully encrypted data communications protocol. Unencrypted ASCII text or similar data transmissions are not acceptable;
 - lvi. All communications between the IFCs and the remote devices must be check-digit coded to protect data from manipulation during transmission;
 - lvii. All communications links between the IFCs and the remote devices shall be monitored such that an alarm is raised at the central control if the data being transmitted is corrupted or tampered with in any way;
 - lviii. All data communication between IFCs shall be encrypted using an industry standard symmetric encryption algorithm equivalent to 256-bit AES or stronger;
 - lix. All data communication between IFCs shall use an industry standard asymmetric encryption algorithm for mutual authentication and session key negotiation. This algorithm shall be equivalent to 1024-bit RSA or stronger. Session keys shall be re-negotiated on a regular basis at intervals no longer than 30 hours;
 - lx. Communication between IFCs and downstream devices shall support a high-speed protocol of at least 1Mbit/second;
 - lxi. The IFC shall support up to 10 high speed communication ports;
 - lxii. The IFC shall support up 80 devices comprising a combination of readers, I/O devices and sensors;
 - lxiii. The IFC shall not necessarily support 80 devices of one type;
 - lxiv. Devices connected to the high communication speed port shall contain a unique serial number;
 - lxv. When connected to an IFC, the serial number of the device shall be reported to The System;
 - lxvi. Once assigned to a function within an IFC, if any attempt is made to substitute readers in the field without authorisation, an alarm shall be generated;
 - lxvii. The IFC shall support the Wiegand connections protocol, supporting up to 65,535 Bits;
 - lxviii. The IFC shall have Open Supervised Device Protocol (OSDP) reader support;
 - lxix. The system shall provide relay output facilities that are system activated in response to alarm activations. Relay functions required are:

- lxx. Activate and latch a relay in response to an alarm. Relay to remain latched until alarm processed;
- lxxi. Activate a relay for pre-set 'pulse' time. The relay to release after the 'pulse' time lapse;
- lxxii. Relay activation to 'mirror' or 'follow' the alarm input activation.
- lxxiii. The system shall incorporate relay outputs that can be activated according to time schedules, rather than alarm event. These outputs may be used to control lighting, heating, or to electronically lock or unlock non-monitored doors.

9 Access Control System Requirements

9.1 Door Control

Access control for a door shall as a minimum provide, however not be limited to the following;

9.1.1 Reception access general:

- i. Access Control reader;
- ii. Emergency release switch input;
- iii. Reception control switch input.

9.1.2 Egress control

Egress control for doors shall allow for the following features where specified:

- i. Exit reader;
- ii. Push button request to exit;
- iii. Emergency exit break-glass.

A push button request to exit shall record the exit in the event database. When requested by a valid means of access or egress, the door shall unlock for a pre-set period, after which the door shall relock. If access or egress is completed prior to the pre-set time expiring, then the door shall relock immediately the door has closed.

The period of unlock shall be extended should a cardholder have a suitable privilege. This may be the case for a person with a disability.

9.1.3 Door Operation Monitoring Recording

All entry and exit methods shall be recorded in the event database. The door shall be monitored for both door open/closed, and door unlocked/locked using concealed monitor switches appropriate for the door installation.

- i. Where the door is a double door, the inactive door leaf shall also be monitored for door open/closed and door unlocked/locked. The inactive leaf door monitor switches may be connected as part of the active door leaf monitoring.
- ii. It shall be the Contractor's responsibility to configure the door in a way that generates a forced door alarm should the door be unlocked and/or opened without first being released by the system. Should a door be left unlocked or open after a pre-set time, an alarm shall be generated reporting the condition.

- iii. Should a valid request to access a door be generated and access not taken, it shall be possible to ignore the request (not record it as an entry event) and automatically re-secure the door after a pre-set time.
- iv. When a valid access through a door is undertaken, the door shall immediately re-secure on re-closing irrespective of the door unlock time.
- v. The system shall have a 'lockdown' feature whereby cardholders who would usually have access to Access Zones are denied access. It shall be possible to 'lock-down' an Access Zone based on any event within the system.

10 Door Register

The following door register provides the minimum requirements per door types as identified within the Design Brief and supporting Drawings. It shall be the Contractors responsibility to confirm all details and provide any additional infrastructure as required to deliver to the client the stipulated operational conditions.

Door/Gate/Roller Shutter Type	Description
DT01	Single door, Single Access control reader, Electric Mortice lock, configured free handle egress, forced door monitoring, Cable transfer and flush reed switch.
DT02	Single door, Single Access control reader, Electric Mortice lock, Request to Exit Button (REX), forced door monitoring, Cable transfer and flush reed switch
DT03	Single door, Dual Access control reader (in/out), Electric Mortice lock, forced door monitoring, Cable transfer and flush reed switch. (BGU)
DT04	One and a half leaf door, Single Access control reader, Electric Mortice lock, configured free handle egress, forced door monitoring, Cable transfer and two flush reed switches.
DT05	One and a half leaf door, Dual Access control reader, Electric Mortice lock, forced door monitoring, Cable transfer and two flush reed switches. (BGU)
DT06	Double door, Single Access control reader, Electric Mortice lock, configured free handle egress, forced door monitoring, Cable transfer and flush reed switch.
DT07	Double door, Dual Access control reader, Electric Mortice lock, forced door monitoring, Cable transfer and flush reed switch. (BGU)
DT08	Single door, Single Access control reader, Electric Strike and flush reed switch, configured free handle egress.
DT09	Single door, Dual Access control reader (in/out), Electric Strike and flush reed switch, Request to Exit Button. (BGU)
DT10	One and a half leaf door, Single Access control reader, Electric Strike, Cable transfer and two flush reed switches, configured free handle egress.
DT11	One and a half leaf door, Dual Access control reader, Electric Strike, Cable transfer and two flush reed switches (BGU)
DT12	Double door, Single Access control reader, Electric Strike, Cable transfer and flush reed switch
DT13	Double door, Dual Access control reader, Electric Strike, Cable transfer and flush reed switch. (BGU)
DT14	Single Sliding Door, Single Access control reader, Electric opening interface, Open state monitoring, Request to Exit Button (REX) (BGU)
DT15	Single door, Single Access control reader, Mag Lock, flush reed switch and Request to Exit Button. (BGU)
DT16	Single door, Dual Access control reader (in/out), Mag Lock, flush reed switch and. (BGU)
DT17	One and a half leaf door, Single Access control reader, Mag Lock, two flush reed switch and REX (BGU)
DT18	One and a half leaf door, Dual Access control reader, Mag Lock, two flush reed switch and (BGU).
DT19	Double door, Single Access control reader, Mag Lock, two flush reed switch and REX. (BGU)
DT20	Double door, Dual Access control reader, Mag Lock, two flush reed switch and REX. (BGU)

GT1	Sliding Gate, Single Access control reader, Sliding Gate Motor interface
GT2	Person Gate, Dual Access control reader, Locking Device to be proposed by Integrator, Open State Monitoring, Fail Secure
RT1	Roller Shutter, Single Access control reader, Electric Motor interface, and heavy-duty roller shutter reed switch
RT2	Roller Shutter, Dual Access control reader, Electric Motor interface, and heavy-duty roller shutter reed switch

All perimeter / egress doors that are external or within an egress path that are identified as fail safe shall be fitted with Break Glass Units (BGU).

11 Uninterruptable Power Supply Units (UPS)

All supporting non-battery backed up equipment and related Network Switch equipment that is not supported by MQU's UPS solution shall have its own dedicated UPS.

The UPS equipment must be of proven quality from well-known and established manufacturers and local established distributors with local spares and engineering support readily available.

All UPS equipment must comply with the requirements of Australian Standard 62040.1:2003; 62040.2:2001 and this Specification. Units must be installed in secure locations.

Each UPS must be sized to accommodate the power requirements of the connected equipment plus an additional 25%, at Practical Completion.

11.1 General UPS Requirements

The UPS equipment must:

- i. Be a True On-Line, Double Conversion unit with the load permanently running from the inverter to supply continuous clean sine wave power;
- ii. Incorporate a network management card for environmental monitoring;
- iii. Be a rack mounted modular unit with provision for external rack mounted battery enclosures. All necessary rack mounting kits, brackets and fixings to suit the existing rack must be supplied with the UPS;
- iv. Provide continuous, clean and reliable no-break 240VAC 50Hz power;
- v. Incorporate over-current protection to prevent damage caused by an inadvertent or malicious short circuiting of the output supply;
- vi. Be designed to enable the connected batteries, when discharged, to be fully recharged in not more than twenty-four (24) hours. This must in no way affect the ability of the power supply to fulfil its normal system operating requirements;
- vii. Incorporate a serial/USB connection between the UPS and the server/storage array, to signal the requirements for the orderly shutdown of the server in the event of a power outage beyond the backup duration of the UPS. Supply the interconnecting cable and any software required to perform this function;
- viii. have the ability to automatic scheduled periodic testing of batteries with battery test failures being reported as an alarm;
- ix. Provide front panel power, inverter and battery status indicators;

11.1.1 UPS Batteries

- i. STANDARDS: To AS 1981 and AS 2676;
- ii. REQUIREMENTS: Provide a battery system having an operating life 3 – 5 years within the specified environmental conditions and suitable for operation in the specified UPS system. Batteries must be housed within matching purpose-built cabinet(s);
- iii. CONTROL: Control the operation of the battery within the UPS system with switches and contactors, rated to the battery fault level and backed up by suitably rated HRC fuses or circuit breakers;
- iv. BATTERY: Sealed lead acid or gel-cell levels: 1-hour rate;
- v. Battery rating temperature: 25°C;
- vi. CAPACITY: Sufficient to provide the rated output from the UPS for the specified period of support time 30 minutes;
- vii. CONNECTIONS: Provide conductors of adequate cross section for mechanical strength and minimal voltage drop for connection.

12 Contractor Requirements

The Contractor is required to:

- i. Utilise the existing Gallagher Access Control and Security Solution and all associated control equipment, transmission devices and associated network cabling in reference to the Universities Design Brief and Drawings;
- ii. All equipment and materials used shall be standard components, commonly manufactured and utilised in the Manufacturer's system, no proprietary hardware or software will be accepted. By proprietary this means that no hardware or software shall be used in the system that can only be sourced from a single Contractor;
- iii. Should additional racking be required, the Contractor shall provide and install MQU approved racking within the nominated locations. Racking shall be suitable to house all the additional equipment controls and terminations for the solution including all additional transmission equipment such as fibre, switches etc;
- iv. The system shall interface with Macquarie University's Security Network fibre optic backbone, as approved by MQU's authorised representative;
- v. When CAT 6e installations are used, attention must be paid to ensure the distance does not exceed 90 metres and is compliant with ICT requirements in respect to distance, quality of installation and performance;
- vi. The contractor shall be responsible for all additional licensing costs, and associated equipment to connect the new components and systems to MQU's Gallagher Head End solution as stipulated in the design brief;
- vii. Working with the University's authorised representative, program, name and allocate all Access Control and Electronic Security infrastructure to the Gallagher Head End system;
- viii. It shall be the Contractor's responsibility to install the new Access Control and Electronic Security system (ISMS) and connect the solution to the Security Network at the designated demarcation points as stipulated in the design brief,

with the final location to be agreed upon by the universities authorised representative.

13 Power

Power to all field devices shall be the responsibility of the Contractor. Power to controllers and readers alike shall be delivered via power supplies with battery back-up and associated devices located within the designated communication rooms. These power supplies shall be hardwired into an electrical junction box. Plug Packs that plug directly into power outlets that can easily be tampered with or turned off will not be accepted.

14 Cabling

Security Network cabling to the designated connection points will be provisioned by the University. The contractor shall be responsible for any additional cabling works from the connection/termination points (equipment rooms) to the in-the-field ISMS devices. In the event that Macquarie University includes any Security Network cabling into the design brief and scope of works, the contractor shall adhere to the following;

- i. Cabling between buildings, floors, hubs and ISMS devices locations on the Campus is the responsibility of the Contractor. However, it should be noted where applicable, Macquarie University may or may not have available existing or adjoining cable tunnels, trays, conduits, ducts or pits / cupboards in place between the various buildings, floors or locations;
- ii. The Contractor is to ensure all communication cabling between buildings, floors or locations is undertaken in accordance with relevant current Australian and Macquarie University General Cabling Specification Standards;
- iii. All wiring is to be neatly loomed and all cables labelled and tagged. Additional "spare" cabling length should be neatly loomed and situated within the confines of duct, conduit or other appropriate protective shrouding, cabinets, trays or pits/cupboards;
- iv. Cable continuity - Unless unavoidable due to length or difficult installation conditions, all cables shall be installed without intermediate joints. All approved cable joints must be soldered and surrounded with heat shrink plastic or through approved patch or repeater panels. The preference is to not have cable joints; however, where joining of cables is unavoidable, the Contractor must provide details pertaining to locations and show the same in associated site plans, system schematics and as built drawings;
- v. Where possible all cabling should be concealed by running through ceiling spaces or wall cavities, all ceiling cables shall be installed in appropriate trays or mounts so that they are supported off the ceiling.
- vi. Where cabling does not run via ceiling spaces or wall cavities, it shall be provided mechanical protection in the form of surface conduit. The conduit shall be securely fastened to the building / structure or fencing with double conduit saddles or, fastened with UV tamper proof fasteners at centres not exceeding 600mm;
- vii. Subject to permission from the University, catenary cabling may be permitted on Campus buildings for power cabling, device cabling and all other network cabling. Strict conditions shall apply for the use of these catenaries, with each application requiring the contractor to seek approval prior to the implementation;

- viii. All SYSTIMAX (CommScope) Cat 6A. Cable selection shall take into account the cable quality and its compatibility with a suitable RJ45 ensuring that the cable sheath is terminated and housed completely within the structure of the RJ45;
- ix. All Network cabling associated with the project will be run to a demarcation point within the University campus for connection into the University Security network. It will be the Contractor's responsibility to work with the University's authorised representative to agree on the final location.

14.1 CAT 6 Specifications

- i. SYSTIMAX (CommScope) Cat 6A Giga SPEED X10D 1091B ETL Verified Category 6A U/UTP Cable, slate jacket, 4 pair count; U/UTP (unshielded) 23 AWG, Diameter Over Jacket 7.239 mm, Jacket Thickness 1.295 mm c);
- ii. ANSI/TIA Category 6A, Characteristic Impedance 100-ohm, Characteristic Impedance Tolerance ± 15 -ohm, dc Resistance Unbalance, maximum 4 %, dc Resistance, maximum 7.61 ohms/100m;
- iii. Mutual Capacitance 6.0 nF/100 m @ 1 kHz, Nominal Velocity of Propagation (NVP) 65 %. Operating Frequency, maximum 550 MHz. Operating Voltage, maximum 80 V;
- iv. Transmission Standards ANSI/TIA-568-C.2 | ISO/IEC 11801 Class EA. Dielectric Strength, minimum 1500 Vac | 2500 Vdc;
- v. Environmental Space Non-plenum. Flame Test Method CMR. Installation Temperature 0 °C to +60 °C. Operating Temperature -20 °C to +60 °C. UL Temperature Rating 75 °C.

15 Conduit and Ducting

15.1 Conduits

- i. Where conduits, ducts etc. pass through damp courses, fire barriers, vapour barriers and the like, damage to these surfaces shall be kept to a minimum and the surface restored;
- ii. Conduits shall be of minimum size 20 mm diameter and shall be run so as to enable cables to be "drawn-in" after erection, sufficient accessible junction boxes to be used for this purpose;
- iii. Except when used in accessible surface runs of conduit to facilitate the running of such conduits around beams and other exposed structural members, inspection fittings are NOT acceptable as a draw in point;
- iv. The direction of conduit run shall be parallel to the walls, floors and ceilings, wherever practicable;
- v. Conduit shall be installed so as to avoid all mechanical duct systems and other pipe systems and services, and shall, in all cases, be at least 75 mm from heating pipes, and at least 500 mm from boilers or furnaces;
- vi. The Contractor shall be responsible for the true horizontal or vertical installation of all boxes and fittings. Where possible conduits shall be run concealed;
- vii. Conduits shall be secured to exposed structural steel members by means of clamps, the drilling or welding of structural steel will not be permitted.

15.2 Steel Conduit

- i. Steel conduit shall be manufactured in accordance with AS-2052;
- ii. All burrs shall be removed from ends and screwed bushes shall be fitted to the ends of conduit runs;
- iii. All conduits shall be straight, free from rust and scale and any sets shall be made cold in such a manner as not to distort the walls of the conduits;
- iv. No threads shall be visible after erection other than running joints;
- v. Running threads of galvanized conduit shall be thoroughly painted with aluminium paint.

15.3 Rigid UPVC Conduit

Rigid UPVC conduit and fittings shall be in accordance with AS-2053;

- i. All joints shall be cemented with approved cement and fittings shall be of rigid UPVC;
- ii. Rigid UPVC conduit shall be securely fastened with approved UPVC saddles at a maximum spacing of 500mm. Where necessary to eliminate sagging in the conduit additional saddles shall be provided. Where rigid UPVC conduit is installed across rafters or joist in roof spaces, it shall be fastened to the side of a timber batten to approval;
- iii. Where any straight section of rigid UPVC conduit exceeds 4m in length an approved expansion joint shall be provided for each 4m or part thereof along the entire length of the straight section;

15.3.1 UV Resistant UPVC Conduit

UV resistant UPVC Conduit shall be installed in the following Locations;

- i. Exposed to mechanical damage;
- ii. Exposed to direct sunlight;
- iii. Exposed to temperatures exceeding 60 degrees Celsius.

15.4 Flexible Conduit

Flexible metallic conduit shall as a minimum include an approved flexible rubberised anaconda;

- i. Flexible PVC conduit may be used in minimum lengths for connections to individual items of plant. These lengths shall be terminated at each end with approved terminating connections.

15.5 Ducting

Ducting shall be approved square or rectangular section PVC or folded zinc annealed sheet steel painted to approval;

16 Fixings to Walls

All fixings of equipment to walls, ceilings, etc. shall be by one of the following means;

- i. Into brick or concrete, by means of approved expanding metal fixings, or by means of expanding nylon fixings;

- ii. Into other surfaces by means of metal toggle bolts or expanding nylon fixings.
- iii. Expanding nylon fixings shall NOT be used for the support of heavy equipment or in areas of high temperature fluctuation;
- iv. Wood plugs shall not be used.

17 Fastening

All fastening of equipment shall be secure and mechanically sized to suit conditions of weight, shape, location, loading and to ensure rigidity. Where proprietary equipment is installed the fastening shall be to the manufacturer's recommendations;

Unless specifically stated otherwise fastening shall be;

- i. Corrosion resistant expanding masonry anchors or plated wood screws into expanding nylon plugs for solid brick or concrete
- ii. Plated toggle bolts (spring loaded or gravity type) for solid hollow sections
- iii. Holes drilled for plugs and masonry anchors shall be sized to the manufacturer's recommendations; plugs and anchors shall be flush with the surface when inserted and fixed;
- iv. Any system equipment or infrastructure, located outside of the building perimeter, shall be secured using anti-tamper screws, fasteners and secured locking systems;
- v. Explosive type fasteners shall not be permitted.

18 Penetrations

- i. The Contractor is to provide for all penetrations, core holes, trenches, and associated civil installation works if required. Written approval is to be obtained prior to the cutting or drilling of penetrations through building structural fabric, membranes, fabric/walls, floors and or ceilings. Make good and seal all penetrations as required and appropriate inclusive of the re-instatement of any fire rating;
- ii. Cables not enclosed in conduit must be provided with UPVC sleeves formed from pipe sections, for penetrations through floor slabs, beams, and external walls;
- iii. Fire rated building elements - Seal penetrations using systems compliant with Australian Standards AS-4072.1;
- iv. Non-fire rated building elements - Seal penetrations around conduits and sleeves. Seal around cables within sleeves. If the building is acoustic rated, maintain the rating;
- v. Membranes - If approval is given to penetrate membranes, provide waterproof seal between the membrane and the penetrating components.

Note - All penetrations must be sealed to ensure compliance with fire standards are achieved. It is the Contractors responsibility to coordinate and pay for the re-certification of all penetrations (applicable to the works performed). The Contractor must utilise the nominated "incumbent" fire company / certifier for recertification works and services.

19 Make Good & Clean Up

The making good of disturbed surfaces will be the responsibility of the Contractor. Should the Contractor, due to the current state of repair of the building/site be concerned that Make Good obligations may be extended beyond that of any direct or indirect works undertaken by the Contractor, the Contractor shall photograph the state of repair of the building prior to commencing work and issue a copy of this photographic record through to the nominated client representative or its authorised representative.

19.1 Debris

- i. All debris such as packaging, metal swag, wire cut-offs produced as a result of the works must be removed from site;
- ii. Equipment cabinets, housings and any associated equipment must be kept clear of wire cable off cuts, metal swag, or debris during the construction phase and completion of the installation works;
- iii. All trade wastes and debris which may obstruct vehicles or persons from reasonable movement throughout the University Campus shall be removed at the end of each day. It shall be the contractor's responsibility to ensure the safety of all person on-site at all times;
- iv. Asbestos: Prior to any work on any buildings, the contractor must consult with MQU Property to access and review the asbestos register. The asbestos register will provide contractors with information where asbestos may be found or is likely to be found on site, or within University buildings;
- v. Work must not be undertaken on any asbestos containing material (ACM) where works such as drilling, grinding or otherwise may release asbestos fibres into the atmosphere;
- vi. Where ACM is found or suspected to be found, the contractor must cease work immediately and contact Macquarie University Property's authorised representative for advice and further assessment prior to proceeding.

20 Labelling

- i. The Contractor shall be responsible for labelling each cable, patch panel, port and LAN jack etc associated with the system. Each field device i.e. reader, strike, network switch(s), hub and power supplies etc, shall be clearly label with an identifying location/number;
- ii. The contractor shall supply samples of labels for all components of the system for approval prior to installation;
- iii. All cables used for the system shall be labelled at each end;
- iv. Labelling schedules shall be prepared specifically for the project and included in the as installed information;
- v. All field devices must be labelled to match architectural room or area numbers. This labelling is to be consistent across the ISMS;
- vi. All labels shall be Traffolyte type printed using black text on a white background;
- vii. All network and field device cabling shall have self-laminating labels at the beginning and end of the cable. Cable Clip style devices for numbering shall not be permitted.

21 Equipment Enclosures

- i. All equipment mounted within any enclosures shall be installed to meet the manufacturer's recommendations;
- ii. All cabling within each enclosure shall be trunked within duct. No equipment shall be mounted on the enclosure door;
- iii. All cable penetrations shall have proper glands fitted and shall be fitted in such a way as to not allow the ingress of rain and water from sprinkler systems etc;
- iv. Each equipment enclosure shall be numbered, and a site location shall be nominated;
- v. Each distribution point for the relevant power feed shall also clearly be identified.

22 Fire Rating and Safety

Where installation works involve coring, boring, chasing or other disruption of fire rated surfaces or systems including doors, wall, ceiling or the like, the Contractor will be responsible for re-certifying through an authorised certifier that the works have not deteriorated the fire integrity of that building element.

The Contractor must advise Macquarie University or its authorised representative in writing of any known or identified areas where any such breach or threat of breach may exist in relation to fire rating or safety standards that are not part of the Contractors direct or indirect works.

23 Workmanship

Equipment shall be installed in accordance with this specification and manufacturer's recommendations, and the accepted principles of sound and safe work practices

24 Licences Certifications

24.1 Security Licences

The Contractor shall hold a current Master Licence under the Security Industry Act for the state of NSW. All operatives performing security related work under the control of the Prime Contractor shall hold a relevant current licence under the Security Industry Act.

24.2 Other Licences and Certifications

All Contractors performing works must hold all the relevant licences and certifications associated with the work being carried out, such as ACA Cabling Licence and ISMS certification. The contractor as part of their submission shall provide all staff licences and certifications prior to the commencement of works including any registration details, as well as providing any details during the project's life-cycle upon request by the University.

25 Health and Safety

All Contractor shall be Cm3 certified ensuring that the obligations imposed by all Health and Safety Legislation, Acts, Regulations and Codes of Practice are complied with at all times, including, however not limited to the following:

- i. Being familiar with the requirements of those Acts, Regulations and Codes of Practice as applicable to the works;

- ii. Ensuring that the specified works provides for the safety of all personnel during installation, inspection, testing and subsequent operation of the system/s;
- iii. Provide input into a site risk assessment to identify hazards, assess risks, and implement risk control measures;
- iv. Provide advice as to all potential hazards not adequately protected to the requirements of the Health and Safety Legislation, Acts, Regulations and Code of Practice;
- v. Provide all temporary or permanent screens, guarding, access buildings, safety notices, identification labels and safety clothing, footwear and equipment required for the execution, testing and maintenance of the works;
- vi. Should hazardous materials be present or encountered, immediately notify the party responsible for site safety, of the location and any details prior to any handling or removal of hazardous materials.

Contractors tendering for the work will be required to complete the University WHS (Work Health and Safety) pre-qualification questionnaire and submit evidence documents including Insurance Certificates of Currency and Safe Work Methods Statements.

26 Warranty

Warranty of all products and installation shall be one (1) year for all parts and labour from the date of acceptance of the system by the University's representative.

27 Maintenance

- i. The installed system shall be subject to twelve (12) months operational maintenance commencing from the date of practical completion. The sites will be deemed to be operational once practical completion is reached and operational monitoring begins, whereby the system shall be checked. A maintenance report shall be completed and submitted to the University for assessment;
- ii. Two periodic maintenance visits are required during the first 12 months with the final visit two weeks before the end of the DLP period. All devices will be tested at each visit resulting in every device in the entire system being thoroughly tested (where accessible) consistently the end of the DLP;
- iii. During each test the Contractor will be required to attend site and confirm the system including each in-the-field device is fully functioning. During these maintenance inspections the service provider shall apply appropriate testing methods to establish the correct operation of each piece of equipment and keep accurate records of all tests and provide Macquarie University with comprehensive reports detailing attendance, actions taken and outcomes within 7 days of attendance;
- iv. Tests are to be carried out during normal office hours and in the presence of the nominated authorised person.

28 Drawings and Manuals

The Contractor shall supply 2 hardcopy manuals, along with associated electronic files, detailing the following:

- i. As built drawings identifying the location of all system components, the location of points of communications connectivity, and the approximate route of system cables;
- ii. Operator instructions including sufficient detail to operate the system (both locally and remotely), configure system parameters, and diagnose system faults;
- iii. The manual shall cover system maintenance including frequency and specific work details.

29 Commissioning and Acceptance testing

- i. The Contractor shall be responsible for all final testing of the systems. The testing shall be performed by the responsible contractor in the presence of the University's representative, and shall include fully qualified representation by the Contractor;
- ii. Unless otherwise noted in these documents, there shall be two inspections, with the first being termed as a preliminary inspection. Prior to this inspection, the Contractor shall provide all documents outlined in these documents. A list of items to be corrected will be developed during the preliminary inspection (punch list);
- iii. The preliminary inspection must occur prior to substantial completion of the system with the final inspection no later than seven (7) days prior to final acceptance in order to meet the University's timetable for systems familiarisation. All these times shall apply unless noted in a specific sub-section;
- iv. The Contractor shall include the cost of these tests and adjustments in his bid proposal and shall furnish all equipment necessary and perform all work required to determine or modify the performance of the System in accordance with the Contract Documents.

30 Training

- i. As requested, the Contractor shall provide operator training for end users, including local users and remote operators ;
- ii. The training shall be conducted for a minimum of 2 hours by a suitably qualified workplace trainer and be delivered in a structured manner including the provision of tutorial handouts with comprehensive system indexing.

31 Safety & Environment

Prior to the commencement of any project, the Contractor is required to complete and submit the following form.

WHS & Pre-Qualification Questionnaire and Review form				
Company Name:		ABN:		
Address:		Phone:	P.	

			M.	
Contact Person:		Position/Title:		
		Date:		

32 Instructions:

To be completed by a PCBU (a person conducting a business or undertaking i.e. the contractor) tendering for contract work or currently contracted by the University.

- Where you see ↴ please attach a copy/sample.
- Where you see ↻ please provide further detail in section 7.

1. External Certification: is the PCBU externally certified to:		Yes	No	Certification no
↴	1.1 OHSAS 18001:2007			
↴	1.2 AS/NZS 4801:2001			
↴	1.3 AS/NZS 14001			






- If all answers in 1 are “no” continue to section 2.
- If one answer is “yes” continue to section 7.

2. Does the PCBU have a written work health and safety management plan that includes: <i>(↴ please provide this plan or the elements listed below)</i>		MQ use only	
2.1	Health and Safety Policy		
2.2	Rehabilitation and Return to Work Policy Plan		
2.3	Consultation arrangements		
2.4	Clearly defined health and safety responsibilities for all members of staff		
2.5	Health and safety criteria when selecting contractors (<i>e.g. provision of safe work procedures</i>)		

2.6	Risk management process <i>(e.g. conducts risk assessments, uses hierarchy of controls)</i>		
2.7	Fitness for work rules <i>(e.g. no drugs & alcohol in the workplace)</i>		
2.8	Procedures for reporting hazards & incidents & conducting investigations <i>(e.g. hazard rpt. form)</i>		
2.9	Procedures for dealing with medical and other types of emergencies <i>(e.g. injury, fire)</i>		
2.10	Procedures for notifying injuries and illnesses <i>(e.g. injury register)</i>		
MQ use only. Reviewed by:		Date:	

3. Does the PCBU have a written environmental management plan that includes: (<i>please provide this plan or the elements listed below</i>)		Yes	No
		MQ use only	
↳	3.1 Environment or Sustainability policy		
↳	3.2 Clearly defined environmental responsibilities for all levels of staff and decision making		
↳	3.3 Identifying, assessing and managing environmental risks		
↳	3.4 Current Aspect and Impacts register		
↳	3.5 Procedures for: minimising waste and emissions; efficient use of energy and resources		
↳	3.6 Environmental criteria when selecting contractors (<i>e.g. provision of Aspect & impacts register</i>)		
↳	3.7 Procedures for notifying and dealing with environmental emergencies (<i>e.g. spill</i>)		
MQ use only. Reviewed by:		Date:	

4. Does the PCBU have safe work method statements for high risk and hazardous work :		Yes	N/A
⚡	4.1 Involving Asbestos		
⚡	4.2 Performed near chemical, fuel or refrigerant lines		
⚡	4.3 Performed in confined spaces		
⚡	4.4 Performed near or in contaminated or flammable atmospheres		
⚡	4.5 Involving the demolition of an element of a structure that is load-bearing or related to the physical integrity of a structure		
⚡	4.6 Involving diving and/or carries the risk of drowning in water or other liquid		
⚡	4.7 Performed near or on energised electrical installations or services		
⚡	4.8 Requiring excavation of a shaft or trench greater than 1.5 metres or a tunnel		
⚡	4.9 Involving the use of explosives		
⚡	4.10 Involving a risk of a person falling more than 2 metres		
⚡	4.11 Involving the movement of powered or mobile plant.		
⚡	4.12 Performed on or near pressurised gas distribution mains or piping		
⚡	4.13 Involving structural alterations or repairs, or involving tilt-up precast concrete		
⚡	4.14 Carried out in an area in which there are artificial extremes of temperature		
⚡	4.15 Exposing workers to traffic: road, railway or other		
⚡	4.16 Exposing workers to noise		
⚡	4.17 Involving manual handling.		

5. Training, Competency and Plant		☐☐☐	No	N/A
	5.1 Is health and safety training provided for specific work activities? (<i>“yes” provide details</i>)			
	5.2 Are records kept of all training & induction programs undertaken by workers?			
	5.3 Are copies of licences kept on file for tasks/undertakings that require a licence?			
	5.4 Is a register of plant/equipment submitted to the regulator where required? (<i>e.g. tower cranes, lifts, building maintenance units, mobile cranes with safe working load >10 tonnes</i>)			
	5.5 Is there a system in place to monitor and maintain plant/equipment? (<i>e.g. daily checks</i>)			

6. What methods of consultation and communication are used by the PCBU?	
<input type="checkbox"/>	Health and Safety Committee
<input type="checkbox"/>	Health and Safety Representatives
<input type="checkbox"/>	Toolbox meetings
<input type="checkbox"/>	Other arrangements (<i>please specify</i>)

7. Further Information: input the reference in the column provided	

8. Insurances			
1	8.1 Name of Public and Product Liability insurer:		
	Policy No:	Expiry Date:	Value of Cover: \$
1	8.2 Name of Workers' Compensation insurer:		
	Policy No:	Expiry Date:	Value of Cover: \$
1	8.3 Name of Professional Indemnity insurer:		
	Policy No:	Expiry Date:	Value of Cover: \$

9. Has the PCBU had any enforceable undertakings issued by the Regulator? <input type="checkbox"/> Yes, <input type="checkbox"/> No	
<i>If "yes" please provide details</i>	
10. Has the PCBU had previous fines, prosecutions, improvement notices issued by the Regulator? <input type="checkbox"/> Yes, <input type="checkbox"/> No	
<i>If "yes" please provide details</i>	

MQP use only

11. Assessment Criteria	
WHS Mgt Plan	<ul style="list-style-type: none"> -WHS policy signed by senior manager demonstrates commitment to WHS - Procedures outline the process to identify hazards, control risk, use of hierarchy of controls - Evidence that the PCBU undertakes risk assessments - Emergency procedures outline the process for incident management (<i>e.g. first aid, fire</i>)
SWMS	<ul style="list-style-type: none"> - Are task specific, job specific & are completed for all high-risk construction work - Identify the steps for the task, the potential hazard & suitable controls
Insurances	<ul style="list-style-type: none"> - Minimum \$10million required for Public and Professional Indemnity Insurance small contracts - Larger contracts: insurance levels need to be linked to the value and risk of the contract

Review by 1:		Position/ Title:	
Signature:		Date:	
Review by 2:		Position/ Title:	
Signature:		Date:	
Result	<input type="checkbox"/> Qualify. <input type="checkbox"/> Not Qualified: additional information required. <input type="checkbox"/> Not Qualified. Re-submission required		

Notes:	
--------	--

END OF DOCUMENT