DESIGN STANDARD

H. Security Services

Contents

Revision log

Current issue

H. Security Services - UoA Design Standards. FINAL Version 3, May 2023

Previous issues

Version	Authors	Description	Revision	Date
1.0	BST Australia Pty. Ltd. on behalf of UoA Service Delivery	H. Security Services - UoA Design Standards	DRAFT Version 1	December 2017
2.0	BST Australia Pty. Ltd. on behalf of UoA Service Delivery	H. Security Services - UoA Design Standards	DRAFT Version 2	December 2017
2.0	GHD	H. Security Services - UoA Design Standards	DRAFT Version 3	March 2018
3.0	Infrastructure, UoA	H. Security Services - UoA Design Standards	FINAL Version 6	

List of revised items

Version	Authors	Revised items	Date
3.0	Infrastructure, UoA	Abbreviations, 1.Introduction, 2.General Requirements removed and reference in Vol.A Project Process Checklist	May 2023

Revision management

It is envisaged that revisions to this document will be undertaken at intervals of not more than two (2) years.

Endorsement body

Director of Infrastructure

Owner

Director, Capital Projects Delivery

Contact person

Manager, Capital Project Delivery

Authors and acknowledgements

The Standards have been developed by Capital Projects with the assistance of University of Adelaide staff, external consultants, contractors, and colleagues from other education institutions.

The University conveys its thanks to all parties who have participated in the development, assessment, and review of these Standards.

Abbreviations

(refer –Standard Volume A. Project Process Checklist)

1. Introduction

(refer –Standard Volume A. Project Process Checklist)

2. General requirements

(refer –Standard Volume A. Project Process Checklist)

3. Technical requirements

This section outlines the specific technical requirements for H. Security Services.

3.1 Security contractor

The Security Contractor (Contractor) shall be a specialist security integrator (company). The Contractor shall submit, prior to awarding the contract the following details:

- A list of previous installations successfully completed as evidence of the previous successful installations of similar size and scope, including a summary of the extent of work for each installation and the value of the security installation
- References or contact names and numbers for those sites.

The Contractor must also be formally assessed by the manufacturer as competent to undertake the configuration and integration of the security system(s) to the level required by the application.

Formal notification from the manufacturer shall be provided and included in the submission. Without that assessment and notification, the Contractor shall be deemed to be ineligible to undertake the work.

3.2 Licences and certificates

Where equipment to be supplied requires licensing, those licences shall be submitted prior to Practical Completion. Complete and submit all license applications.

All equipment shall be licensed to the University of Adelaide and not to the supplier/installer of the equipment.

3.3 Technical data sheets

Submit the technical data sheets for all equipment not nominated as part of this specification, for review and approval prior to awarding the contract.

3.4 Contractor's requirements

3.4.1 Equipment quality

All equipment, materials, cabling and ancillary components shall be "new". All product supplied and installed shall be previously unused and carry the full manufacturer's warranty.

3.4.2 Making good

When execution of the Works causes damage, or removal of redundant equipment leaves an unsatisfactory finish, repair such damage or finish with materials compatible with the surrounding material and finished off flush with the adjacent surface.

This shall include, but not be limited to repair or replacement of door frames, doors, re-establishment or making good of all panels, housings, and other areas necessary to be re-established which are in the opinion of the Security Manager, damaged in the course of the Works.

3.4.3 Site inspection

Where work is to be undertaken at an existing facility, a site visit prior to any submission is highly recommended. The Contractor is responsible to be aware of the site conditions to ensure that all work and equipment necessary to complete the installation is included in the offer.

No extra costs will be allowed because of failure to conduct a proper site inspection or for work that does not comply with the referenced documents.

3.4.4 Acknowledgement

A submission will be considered as an acknowledgment by the Contractor that the Contractor has fully ascertained the scope of work required to ensure compliance with all the requirements of the specification, standards and reference documents.

3.5 Mains supplies

Where essential supply is provided, all security equipment shall be connected to the essential supply. A separate circuit (or circuits) shall be provided for the security system.

3.6 Extra low voltage power supplies

3.6.1 General

All power supplies, transformers, and voltage rectifiers required to supply any voltage other than 240VAC (e.g. low voltage power/extra low voltage power) for equipment detailed in the specification shall be supplied and installed as part of the security services scope of Works.

Extra low voltage power supplies shall be self contained and installed within the secure equipment cabinets. The power supplies shall be a switch mode and the battery capacity shall equal at least 8 hours in normal stand-by operation or at least 2 hour for normal access control of entry/exit activity.

All power supplies must have their mains condition monitored and shall activate an alarm on the security system if a problem occurs (e.g. loss of mains).

The University of Adelaide may require the use of linear power supplies in some installations to reduce any possible interfaces to the Facilities electronic equipment used in high technology buildings. This shall be determined by the Security Manager and shall reflect on the supplied drawings. The minimum specifications as above shall be utilised when supplying linear units.

Details must be provided in the material list/schedule of the capacity and type of each power supply included in the design.

3.6.2 Load

The load on each power supply shall be such that 25% minimum spare capacity is provided.

3.6.3 DC power supplies

All DC power supplies shall be the regulated voltage type.

3.6.4 Camera power supplies

All internal and/or fixed CCTV network cameras shall be powered by Power over Ethernet (PoE) and shall be provided by the UofA ITS department.

3.6.5 Access control panels power supplies

Each access control panel shall be powered separately using dedicated extra low voltage power supplies.

Provide a sealed battery and charger system to all doors fitted with electric locks, and as necessary to power all alarm and access control equipment required. The batteries shall be capable of sustaining operation for at least 8 hours in the event of a mains supply failure.

3.6.6 Lock power supplies

All electric locking hardware primary power (i.e. the main low voltage power to the electric mortice lock, electric strike or electromagnetic lock) is included as part of the scope of work.

The scope of work for security services also includes:

- All wiring connections between the lock and all monitoring and control devices;
- Connection of the primary AC/DC power to the electric locks; and
- The provision of any AC/DC power supplies required for signalling control, such as lock/unlock functions.

3.6.7 Labelling

Engrave all power outlets to which security equipment is connected with the words “SECURITY EQUIPMENT - Do Not Switch Off” as 5mm high black lettering. All UPS outlet faceplates shall be RED and engraved “UPS” in 5mm high white lettering.

Coordinate with the electrical contractor to provide labelling at switchboards of all circuit breakers supplying security equipment with the words "Security Equipment - Do Not Switch Off".

3.7 Power supply monitoring

Where a UPS is provided to supply equipment or services required by the specification(s), whether by others or as part of the scope of work of the specification(s), the security system shall monitor the following alarms:

- UPS low battery alarm
- Mains fail alarm
- Generator fail alarm.

3.8 Electromagnetic interference

All equipment is to be protected against mains transients and induced voltage surges. Protective devices matched to the electromagnetic environment shall be used to achieve protection of equipment against surge voltages.

3.8.1 Personal computers (workstations)

PC hardware supplied for any security services system shall be coordinated with the UoA ITS department. The client workstations shall be ITS SOE workstations that meet the performance requirements for both Genetec Security Center and Siemens SiPass.

The CCTV workstations shall run the latest Windows operating system with Genetec Security Center Client Software loaded.

3.9 Server

All servers supplied by the UofA ITS department.

3.10 Software

3.10.1 General

All software updates released within the contract period up to the completion of the defects liability period, shall be deemed to be included in the contract and shall be provided and installed, at no cost.

A copy of all software necessary to re-establish system/sub-system operation after a catastrophic failure, shall be provided to the Security Manager as a deliverable in accordance with this specification. A copy of firmware is not required.

3.10.2 Software requirements

Software supplied shall be:

- The latest version of stable software available at the time of installation (Beta software shall not be provided);
- Non-proprietary (other than the 'core' specialised software code);
- The operating system developer shall offer full support (not 'self help') for the proposed operating system for a minimum of 4-years from the date of Practical Completion;
- The operating system(s) provided shall be suitable for the intended applications for each computer; and
- Constructed/modified to include nomenclature and operating features which reflect the accepted user terminology and operating procedures.

3.10.3 Programming

Carry out programming to meet the University of Adelaide's requirements. Program all equipment supplied including initial set-up and data entry in accordance with the requirements for each user, local/remote operation, or network interface to other systems.

3.10.4 Naming conventions and descriptors

Coordinate all naming conventions and descriptors to ensure that they are consistent.

3.10.5 Completion

All programming shall be completed prior to the commencement of on-site testing. The Contractor shall demonstrate software and programming to the Security Manager one month prior to the commencement of on-site testing.

3.11 Equipment enclosures and cubicles

3.11.1 General

All equipment enclosures for internal use shall provide a minimum of 25% spare capacity for future expansion.

Where necessary, enclosures are to be supplied with rear mounting plates and top entry cable gland plates to facilitate top entry of cables from over-head cable trays, cable ducts or conduits.

Holes provided for cable access shall be suitably protected with grommets to prevent moisture ingress and to provide protection for cables. Screws shall be complete with captive fibre washers. Enclosures shall be securely fixed in position. Each section of cubicle, panel and rack shall be labelled to indicate equipment/device identification and number and local power supply circuit number.

3.11.2 Tamper alarms

All equipment cubicles and enclosures used to house security equipment shall be complete with tamper alarm connected to, and monitored by, the security system.

3.11.3 High Level Interface (HLI) requirements

All HLIs shall be duplex, that is, commands and responses shall be capable of being transmitted and received in both directions simultaneously.

3.12 Security specification - installation

3.12.1 Fit for purpose

The installation shall be fit for purpose. It is not possible within the text of the specification to describe every occasion where the installation practices of an inexperienced Contractor may adversely impact the environment in which the security services are to be installed.

It is expected that every Contractor has appropriate project experience, including installation experience, gained through successfully completing previous projects of a similar scope and complexity, and that the experience acquired shall ensure that the installation complements the 'environment'.

Where a Contractor has not previously completed a project of similar scope and complexity there is an increased risk that the Contractor's knowledge, both practical and intuitive, shall be inadequate, and that situations may arise where the installation is not fit for purpose.

3.12.2 Obvious work

All supplementary miscellaneous items and devices which are incidental to, or necessary for, the complete operational installation as described in the specification shall be provided whether such work is, or is not, specifically shown or specified.

Unless otherwise noted, the drawings are diagrammatic only. All components shall be supplied and installed in a location and manner as necessary to provide the specified function and performance. Where components are shown on drawings those components are generally not drawn to scale and the final position of each component shall be fully coordinated with all other architectural, structural and services elements.

3.12.3 Surge and lightning protection

Provide adequate surge, lightning and transient protection on all systems equipment and hardware installed to meet the requirements of these Works.

Equipment necessary to prevent or minimise damage from power surge to all systems and system components shall be provided as part of these Works.

Particular attention shall be given to all external cabling devices that are interconnected and/or interfaced to the various systems and equipment mounted at high level (e.g. video Cameras mounted at high level).

Protection shall be in accordance with AS/NZ 1768-1991 for the protection of equipment and include both primary and secondary protection and suppression of both differential and common mode transients.

Where necessary, additional earth stakes shall be installed at external locations so that the resistance to earth at any equipment enclosure complies with the requirements detailed in the relevant standard.

All external cabling shall be provided with in-line lightning protection.

3.12.4 Painting

All new metal work, and the rework of existing metal work, shall meet the Australian Standards, including but not restricted to AS1627 and AS3750, for paint and rust work, and be free from grease, rust scale, and shall be finished with an approved factory applied paint system of approved colours.

Paint finish shall include the following:

- One coat of self-etching primer
- One coat of lacquer primer surfacer
- Three coats of lacquer finished to high gloss.

Ensure finished surfaces of all paint work, not otherwise specified, are free from bubbles, runs or any other imperfections and have a high gloss finish.

All touching up of paints shall be accurately matched to the factory applied finish. Alternatively, a powder coat finish may be applied to metal work.

Preparation and application of powder coat finish shall be carried out in accordance with the manufacturer's recommendations and AS4506, with a minimum thickness of 50 microns.

Submit colour and finish sample for comment by the Security Manager prior to implementation.

3.12.5 Wind load

The Security Services Works shall be designed and constructed to comply with the requirements of AS/NZS 1170.2 Wind Loads where applicable.

3.12.6 Vermin and insects

All enclosures, cabinets, ducting and conduits shall be sealed or otherwise protected to prevent the entry of vermin or other insects which could damage the equipment or cabling.

The proposed method for protection against vermin and insects shall be submitted for approval to the Security Manager.

3.12.7 Environmental considerations

Environmental protection shall be provided to all external equipment where that equipment may be damaged by vandalism, or by environmental conditions such as rain and dust.

3.13 Cable installation

3.13.1 Cable supports

All cable installation shall comply with the following:

- In walkway ceilings: dedicated security services cable tray, secured to ceiling with different cable types (e.g. video, control etc) loomed separately within the tray;
- In riser cupboards and risers: dedicated security services cable tray, minimum size 450mm), secured to wall with different cable types loomed separately within the tray.
- Generally in all ceilings: connected to catenary cables except for major cable trunks which shall be supported using dedicated security services cable tray secured to ceiling with different cable types loomed separately within the tray.

3.13.2 Cabling

Cable installation shall comply with the following:

- Run cables in concealed routes. Do not use surface conduit without written approval. Provide cable tray, cable routing and layout management to minimise congestion at entry and exit points to equipment cubicles, equipment racks and 'equipment rooms'.
- Cabling to all Equipment Cubicles and all wall mounted swing racks shall be concealed;
- Exposed cables (interior) – enclosed in PVC conduit except where cables are installed in any external areas of a where cables shall be enclosed in galvanised steel conduit; and
- Cables installed in concrete shall be enclosed in rigid PVC.

3.13.3 Security cabling

All security field devices are to be cabled using manufacturer approved multi-pair multi-strand copper cable (e.g. 14/0.20 gauge cable to devices except power to electric locks which is to be a minimum of 24/0.20 gauge). Electric lock power cabling is to be sized appropriately to prevent voltage loss due to distance.

All security cabling shall be AS/ACIF S008 compliant multi stranded security type cable, installed in accordance with AS 2201.1, Section 7.

3.13.4 Video cabling

See M. Audio Visual Design Standards.

3.13.5 External cables

All external cables for all security services, regardless the type or use of the cable and regardless of the method of installation (e.g. installed in conduits), shall contain an approved waterproofing agent and shall be suitable for direct buried application. Cables designated by the manufacturer 'for internal use' or 'for in-ground, in conduit use' and the like are not acceptable and shall not be provided.

3.13.6 Separation

Provide 150mm separation between Low Voltage (LV) services and security services to ensure that system performance is not adversely affected by interference and the like.

Where necessary provide additional cable tray to maintain the separation requirements. Separation from High Voltage (HV) services shall be 'to approval'.

3.13.7 Joints

No joints or connections are permitted between the two end points of a cable run. Adequate loose cable shall be provided to facilitate inspection, adjustment and removal.

3.14 Conduits and pits

3.14.1 Type

Provide conduits for cable access for cable protection at entry/exit points and penetrations where cable tray is not specified. Provide either UPVC or steel conduits as detailed. All site conduits and pits for security services are included in the scope of Work.

All visible conduit and duct routes shall be identified prior to installation by the Contractor and approved by the Security Manager.

The contractor must supply to the Security Manager Shop Drawings showing the proposed conduit runs. Approval must be granted before commence of work. Any deviation from this shop drawing as part of a project requires consultation and formal agreement from the Security Manager.

3.14.2 Installation

Observe the following points:

- Do not use surface conduit without express written approval
- Where written approval to use surface conduit has been provided, support the surface conduit and fix with saddles spaced no more than 600 mm apart
- Where saddles cannot be fixed to the building structure a suitable bracket shall be supplied and installed
- Provide connecting blocks/mounting plates for the flexible conduit at penetrations
- Paint exposed internal conduits to match the colour of the surface to which the conduit is attached
- Paint exposed external conduits to match the colour of the surface to which the conduit is attached
- Ensure conduits and cables are neat, straight and securely fixed parallel to building members and walls and do not install in shelving and/or cupboards and the like
- Metallic conduit exposed to the weather shall be galvanised
- Provide draw cords in conduits including spare conduits. Leave 1m of cord coiled at each end. Use polypropylene cord or insulated stranded earth wire 2.5 mm2 minimum size

Install conduits far enough above ceilings and below floors to avoid accidental piercing by nails and the like and to avoid restricting the removal of ceiling tiles or floor panels.

Where possible install conduits at least 150mm clear of underside of roof decking.

3.14.3 Internal conduits

3.14.4 External conduit

All conduits installed externally of a building shall be steel conduit (plated or painted depending on environment) to prevent tampering. The conduit shall be secured using full metal saddles, spaced at a maximum of 600mm and at a minimum of 150mm from other fittings.

The conduit shall be installed so that cables can be drawn in at draw boxes only. Inspection elbows shall not be classified as draw points.

The conduit shall be filled with cables to not more than 60% of its capacity.

3.14.5 Cable duct

The cable duct shall be fitted with removable covers.

The cable duct shall be fitted with the manufactured standard bends, elbows, couplings and reducers.

The cable duct shall be manufactured from extruded PVC when exposed. Concealed cavities and ceiling spaces maybe metal.

The cable duct shall be filled with cables to not more than 60% of its capacity.

Cable duct shall not be used on external building installations.

3.14.6 Fixings

Fixing shall comprise metal thread screws or bolts into expanding type masonry anchors for fixing to concrete or masonry.

Fixings shall comprise tapered woodscrews for fixing to timber (full thread).

Fixing shall comprise metal expanding anchors for fixings to gyprock.

All fixings shall be corrosive resistant.

3.14.7 Cable pits

The Contractor shall provide a system of drained underground pits and conduits:

- To each external and each perimeter equipment enclosures
- For all external underground conduit runs every 50 metres or wherever there is a change of direction
- For the telecommunications carrier services to site
- Elsewhere as detailed

Cable pits shall be heavy-duty concrete pits as detailed on the drawings. Provide pit covers to AS 3996 to suit expected loads. Covers shall be concrete filled cast iron frames. Fit flush with the top of the pit and finish to ground level. The maximum weight of any section of the pit cover shall be 40kg. Provide a lifting handle for each size of cover section, stored in the Security Equipment Room or Communications Equipment Room.

The Contractor shall provide Barri Security bolts. A minimum of two bolts shall be provided for each pit cover. All pit covers shall be keyed alike.

The Contractor shall provide drainage from the bottom of cable pits to the storm water drainage system.

Lay conduits with a drainage fall of at least 1:100 to drain the pit system to the lowest pit or pits. Drain the lowest pit or pits with a 50mm PVC pipe in one corner, with the floor of the pit having a fall towards this pipe. Connect the drain pipe to the stormwater pipe at a lower level than the bottom of the pit to be drained.

3.15 Underground cable routes

3.15.1 Survey

Accurately record the routes of underground cables before backfilling.

3.15.2 Location marking

Accurately mark the location of underground cables with route markers consisting of a marker plate set flush in a concrete base. Place markers at each joint, route junction, change of direction, termination and building entry point and in straight runs at intervals not exceeding 50 metres.

- Concrete bases: 200mm diameter x 200mm deep (minimum dimensions)
- Direction marking: Show the direction of the cable run by means of direction arrows on the marker plate. Indicate distance to the next marker
- Plates: Brass, minimum size 74mm x 75mm x 1mm thick
- Plate fixing: Waterproof adhesive and four brass or stainless steel countersunk screws
- Marker height: Set the marker plate flush with paved surfaces, and 25mm above other surfaces

3.15.3 Marking tape for buried conduits

Accurately mark the location of underground conduits with route marking tape. Provide communications services marking tape and install at the midpoint between the surface and the buried conduit, for the entire length of the conduit run.

3.16 Contractor's responsibility

3.16.1 General

The installation methods, guidelines and standards issued by the manufacturer's/supplier's representatives of the supplied equipment are to be adopted and utilised throughout the contract. All work is to be performed to a level consistent with accepted industry standards of trade practice. Where conflict arises between this specification, the standards and referenced documents, the manufacturer's/supplier's requirements and the industry standards of trade practice, the most stringent requirements shall be applied.

3.16.2 Temporary cabling

Provide temporary cabling and/or equipment to maintain all the systems during any upgrade process. All temporary cabling shall be removed after completion of the upgrade and testing. The disconnection of, removal of, or relocation of any specified items shall be carried out at a time directed by the Security Manager. The Contractor shall provide in writing, to the Security Manager for approval, details of planned interruptions to the services. A minimum of 24 hours advance notification shall be provided.

3.16.3 Maintenance of services

Maintain all existing services at all times. Efficient cutover of services shall necessitate the 'buzzing out' of existing services to determine the nature of the cable allocation, where complete records are not available. Cutover of existing services to the new infrastructure may need to

be accomplished outside normal working hours (i.e. after hours or during weekends). Cutover of services shall be coordinated with the Security Manager.

3.16.4 Redundant cabling and equipment

All redundant cabling and equipment shall be removed and equipment returned to the Security Manager. The Contractor shall provide an inventory of all items including serial numbers. All items shall be suitably packed to prevent damage in transit and all items and packages shall be clearly labelled.

3.17 Identification

3.17.1 Cabling

Identify all cables at all connection points (including marshalling panels such as access control data gathering panels). All connection points shall be uniquely identified and labelled at each end of each cable.

3.17.2 Documentation

The Contractor shall supply documentations shall include as-built drawings, shop drawings, equipment schedules, wiring and system schematics which clearly identify all cable numbers, equipment identification, equipment serial numbers and connection point identification.

3.17.3 Labelling

Label all equipment installed in the equipment racks and equipment cubicles, all wall-mounted panels and all marshalling panels. Labels shall be glue-fixed traffolyte labels engraved with alpha or alphanumeric characters which clearly identify the functions and functional groups. Lettering is to be white on a blue background and affix labels for rack mounted equipment to 1RU blank plates installed in the racks.

3.17.4 Terminology

Standard terminology, generally adopted by the UoA, is to be used throughout.

3.18 Alarm/access control panels

3.18.1 Door controllers and input-output modules

Unless otherwise specified, locate in the respective block or in designated Equipment Cubicles (EC) or 'equipment rooms'. Each monitored device and each controlled device shall represent a separate 'point'. All detection and monitoring devices such as motion detectors and magnetic reed switches shall be individual monitored 'points'.

3.18.2 Installation

Where control and monitoring equipment requires installation in close proximity to the controlled or monitored device, that control equipment is not be installed on ceilings/walls of any room or corridor.

Where equipment cannot be located in designated areas (i.e. designated EC locations or 'equipment rooms') the equipment is to be located in an alternative, concealed, location. The location of these devices shall be identified in the as-installed drawings and in the security manuals. Unless otherwise recommended by the manufacturer all marshalling panels shall be installed in the locations nominated for ECs.

3.19 Door contacts

3.19.1 Magnetic reed switches

Provide magnetic reed switches to all doors as nominated on the drawings. Magnetic reed switches shall operate when:

- A personnel door is opened > 20 mm at the lock/latch edge
- The fixed leaf of a double door is opened > 20 mm at the lock/latch edge
- A vehicular door is opened > 100 mm.

3.19.2 Lock monitoring

Where electric locking devices incorporate integral door, bolt and handle position sensors or magnetic bond sense sensors, these shall be monitored by the alarm/access control systems.

3.19.3 Construction

Provide concealed type magnetic reed switches for pedestrian access doors and heavy duty roller door type magnetic reed switches for larger equipment access doors and roller doors.

3.20 End of line devices

3.20.1 General

End of Line (EOL) devices shall be installed at the security device connection points.

3.20.2 Anti-tamper devices

Provide anti-tamper devices to all equipment cubicles.

3.21 Vehicle control and barrier systems

3.21.1 PE safety beams

The Contractor shall provide a photo electric beam safety interlock to prevent door or gate from closing until the vehicle has cleared the exit point. Provide a separate PE beam transmitter and receiver (i.e. reflective type PE beams shall not be used).

3.21.2 PE beam installation

Installation of the PE beams, logic controllers and reed switches shall conform with the following:

- Where possible, PE beams to be located at 600mm AFFL and 600mm from each side of the shutter opening. Where this cannot be achieved and PE beams are located within 600mm of openings, beams shall be fitted with heavy duty protective shrouds designed to protect beams from vehicle damage and accidental misalignment
- Logic controller to be on the same side as the supply power and installed at a height of 1500mm AFFL
- A conduit is required between the PE beam transmitter and receiver, and from the PE beam (logic controller side) to the logic controller
- A conduit is required for each reed switch cable. Reed switches shall be installed at floor level and within 75mm of the shutter opening.

Confirm details with the Security Manager prior to commencement of construction.

3.21.3 Exit loops

Provide exit loops to operate the roller shutters/boom gates.

3.21.4 Boom gates

Boom gates shall provide the following minimum features:

- Heavy gauge steel housing
- Powder coated finish
- Boom gates shall have a folding aluminium arm to suit the space available but without restricting vehicular access when in the 'open' position
- Direct coupling motor to boom
- Simple interface connection to the Access Control System
- Simple interface connection to the Intercommunication System with remote control capability
- Provide physical restriction to the car park area, through and around the boom gate when closed, to vehicles of width 0.5m or greater
- Open to the vertical position
- Shall be able to be opened by separate momentary action type remote release buttons
- Egress boom gates shall be automatically opened by vehicles leaving the car park by in-ground detection loops
- Shall have manual override (mechanical operation) in case of system failure
- Shall not close on a vehicle under the boom and if partially closed shall return to the vertical position
- Shall close automatically with timeout timer and photo optical obstruction sensor
- Shall be weatherproof and vandal resistant
- Shall incorporate up/down status indicator on the access control system

3.21.5 Roller shutters

The scope of work shall include but not limited to the following:

- Integration of the roller shutter operation with the access control system to provide the monitoring and control functions, including the provision of, and cabling to, the logic controller for connection by the roller door contractor
- The provision of additional equipment as required for interfacing to the roller shutter doors
- Configuration of the system to allow operation of the roller shutters during after hours with the boom gates permanently raised. The reverse shall be provided during normal working hours (i.e. roller shutter up and boom gates controlling access)

- Override to allow the roller shutter to be closed at any time
- Connection of the boom gates and roller shutters to the exit induction loop and provision and installation of the exit loop
- Monitoring the status of the roller shutter

3.21.6 Vehicle exit pedestrian warning

Provide a vehicle exit pedestrian warning system for each egress boom gate/roller shutter that provides vehicular egress across a public pedestrian footpath. The warning system shall consist of an externally mounted rotating orange light and an externally mounted audible alarm. The light shall be installed to provide maximum pedestrian visibility and each audible alarm sound level shall be suitable for intended use. The light and audible alarm shall automatically operate during vehicle egress (i.e. from the time the vehicle reaches the exit loop) and shall continue for a pre-settable duration (minimum duration 10 seconds). The audible alarm level shall be adjustable. The vehicle exit pedestrian warning system shall be interfaced to, and controlled by, the access control system.

3.21.7 Monitoring

Provide Sentrol 2700 heavy duty reed switches (or equivalent) on both internal sides of vehicle doors, which generate a door closed indication at the control panel. All roller doors shall be provided with Sentrol 2700 (or equivalent) reed switches. Provide reed switches to identify the fully closed position.

3.22 Fixed duress alarm system

3.22.1 Type

The fixed duress alarms shall be either:

- Fixed location push button, overt - these shall be wall mounted and visible to all persons
- Fixed location push button, covert - these shall be desk mounted and shall be installed in a concealed location, not visible to detainee or visitors

The type of fixed duress shall be as detailed in the equipment schedule.

3.22.2 Duress buttons

The Duress Alarm push buttons must be:

- Dual- button type, for under bench call points
- Key resettable with reactivation of power by controlled lock out process
- In accordance with Schedule 4.1 Equipment schedule of this document.

3.23 Movement detectors

3.23.1 General

- Install mounting brackets where direct corner or direct wall mounting does not provide optimum PIR detector performance; and
- Wall mounting detectors with a ceiling mount adaptor bracket are not acceptable where ceiling mounted detectors are scheduled.

3.24 Intercom system

3.24.1 General

Intercoms shall be:

- Flush mounted with back-boxes
- Suitably weatherproofed for all external locations and located on external walls or pedestal stands in suitable recessed mounting boxes, which shall include a rain drip cover
- Robust and vandal resistant - all cabling must be installed with adequate extra length to allow complete removal for service access without undue stress on the cabling
- Sealed around the faceplate to prevent the ingress of dust, moisture and the like.

3.24.2 Mounting height

The intercom unit (call point) must not exceed 1400mm to bottom of the unit. Actual height of the intercom unit shall be determined on site.

3.24.3 Weatherproofing

If exposed to the elements, provide a weather-resistant hood above the intercom unit.

3.25 CCTV system

3.25.1 Identification

The Contractor must provide security camera identification so that the camera identification is displayed at every monitor (including playback monitors).

The Contractor must position and aim cameras to provide optimum coverage and to minimise the effect of shadows or direct light sources. Ensure that cameras are installed at a height which will eliminate unauthorised tampering of the camera and associated components.

3.25.2 Fixing

Provide mounting brackets and hardware which rigidly fix cameras, monitors and accessories to buildings or structures. Camera brackets as per camera manufacturer to suit the individual installation requirement.

3.25.3 Surge protection

Surge protection is to be provided by the UofA ITS Department.

3.26 Camera poles and footings

3.26.1 Requirements

The Contractor shall provide camera poles and footings that meet these requirements:

- Circular, hollow, tapered and reinforced rigid concrete poles
- Height 6 metres minimum above ground level
- Poles with internal earth strap (and electrically earthed in accordance with AS3000)
- Poles fitted with a pole cap manufactured from hot dip galvanised mild steel
- Poles with integral mounting attachment for the pole cap
- Pole caps with drilled and tapped mounting holes for fitment to the pole and for fitment of heavy duty camera mounting brackets to the pole cap.

3.26.2 Footings

Footings shall be designed by a qualified Structural Engineer. Submit shop drawings and certification of the pole and footing design, for approval, at least 20 working days prior to the anticipated installation. The design must allow for local soil type and wind loading.

3.26.3 Pole location

Pole locations shall be determined by the field of view requirements as specified. Proposed locations shall be confirmed using a 'cherry picker' (or similar) and a view finder to confirm the field of view. Actual pole heights shall be determined on site to provide required view. The location of poles, shown on the drawings, is indicative only.

3.27 Security specification – technical requirements

3.27.1 Mechanical key locks – general

The UoA uses ProMaster 5, a master keying software program for the management of their master key systems and design.

3.27.2 Master keying system

All UoA key locks shall be Abloy Pro-Tec. The Abloy Pro-Tec lock and master keying system profile shall be ordered directly from the manufacturer and configured to the University's own key profile.

The University of Adelaide Thebarton Campus (nominated areas) use Lockwood Generation Six master keying system with a Thebarton Campus key profile.

The contractor shall liaise with the Security Manager before installing any key locking.

3.27.3 Locksmith

The UoA's locksmith can be contacted via the Security Manager.

3.27.4 Electronic access control system

All access control equipment shall be from the Siemens SiPass Integrated range of hardware unless otherwise advised or approved by the Security Manager.

All electronic locked doors, either internal or external shall be free egress via means of a free handle where electric mortice locks are used or an exit switch for all other lock types.

All building perimeter entry/exit doors shall be electronic access controlled. These doors shall have CCTV coverage.

Each electronic access control door shall provide but not limited to the following:

- Remote control electric locking
- Door status monitoring
- Emergency break-glass door release
- Vehicle access control
- Audible and visual alarms
- Contactless card reader.

The contractor shall provide a Siemens SiPass Integrated electronic security solution. The SiPass Integrated system shall include but not limited to:

- ACC5102 - Advanced Central Controller (ACC)
- ADS5200 - Single Reader Interface (SRI)
- ADD5100 - Dual Reader Interface (DRI)
- ADE5300 - Eight Reader Interface (ERI)
- Power Supply Unit (PSU).

The Contractor must provide to the Security Manager Shop Drawings showing the proposed panel layout and panel locations. Approval must be granted before commencing work.

Any deviation from this shop drawing as part of a project requires consultation and formal agreement of Security Manager.

3.27.5 Access requirements

When the system is activated, access to the building shall be gained by:

- Presentation of a valid card at a reader
- Operation of a remote release button.

Both actions above shall result in the release of the electric door lock for a specified pre-settable time.

3.27.6 Operation requirements

Doors under the control of the Siemens SiPass Integrated system shall be installed and programmed for:

- Forced door
- Door open
- Door open too long
- Lock or bond sense
- Individual break glass alarm.

At the expiration of the door open time an alarm shall be activated at the central SMS.

Should the door be illegally opened, an immediate alarm shall be transmitted to the central processor.

3.28 Door control devices

3.28.1 General

The Contractor shall provide proximity card readers, and locate next to entry/exit points on the opening side of the door. Where the drawings indicate that readers are to be installed in a location other than the door opening side, confirm the requirement prior to commencing installation.

The Contractor shall provide weatherproof external units, if the proximity card reader is mounted external to any building.

Mounting height (pedestrian access): 1.05m if stand-alone, immediately below if combined with the intercom slave unit, or at the same height as other fittings (e.g. light switches) if installed in close proximity.

Mounting height (vehicular access): Generally, 1400mm but to be determined on site, in coordination with the Security Manager.

3.28.2 Access control card readers

Each electronic access control door shall be provided with access control card reader(s).

The access control card reader and its controller shall be intelligent with sufficient memory to store valid key numbers and time zone information to the maximum system expansion capability. The card reader shall operate unaffected when communication with the central processing unit fails. Restoration of the communication link shall result in automatic update of information in both directions. The control

device which directly commands the lock coil shall not be contained within the reader head, so as to preclude the risk of unauthorised access by tampering with the data reader head wiring.

All contactless card readers shall be HID R10 SE Desfire Bluetooth Mini Mullion Reader card readers configured to read the UofA Corporate 1000 card format.

Readers shall be suitable for the installed location. Outdoor type readers shall be used for all external applications. Medium range readers shall be used for all vehicular applications.

3.28.3 Access cards and tokens

All contactless access cards shall be flexible PVC business card sized high security Desfire EV1 type, configured with the UofA Corporate 1000 format and suitable for the application of photo ID.

3.28.4 Break-glass panels

The Contractor shall provide resettable emergency break-glass panels, colour green, at egress doors. The call point shall be cabled in series with the power to the lock. Activation of the break-glass shall report to the access control system.

The break-glass panel shall, when operated, cut power to the door lock and release the door. The call point shall be located at the door position and shall be engrave labelled on the face plate with the words 'Emergency door release. Break glass to activate.' Resetting of the glass shall reset the door.

The power from the door controller to the lock (via the call point) shall also be in series with a normally closed relay contact within the FIP. The normally closed relay contact shall open in the event of an alarm at the FIP and shall only be 'resettable' at the FIP. Coordination associated with the provision of this feature is included as part of the scope of work of this specification.

Specify break glass panel in accordance with Schedule 4.1 Equipment schedule of this document.

3.28.5 Locking general requirements

Engagement with end-users and UoA Service Delivery Manager Security must occur to establish requirements for fail-safe and fail-secure doors. All locks must be fitted with tamper proof screws if on the non-secure side and to include appropriate mounting equipment for inward and outward swing doors.

All electric strikes shall be fitted with a diode across the coil to reduce "Back EMF."

3.28.6 Electric mortice locks

All electric mortice locks shall be as per Schedule 4.1 Equipment schedule.

3.28.7 Solenoid door latch (electric door strike)

All electric door strikes shall be as per Schedule 4.1 Equipment schedule.

3.28.8 Electromagnetic locks

All electromagnetic locks shall be as per Schedule 4.1 Equipment schedule.

3.28.9 Egress door release

For all doors not fitted with an electronic mortice lock, an infra-red (touchless) door release button is to be provided adjacent to the handle side of the door. This switch is to release the electric lock and override the forced door alarm during a legitimate exit through the door. Door release button as per Schedule 4.1 Equipment schedule.

3.28.10 Double leaf doors (solid frame)

The Contractor shall provide an electric mortice lock / electric strike on the non-fixed leaf, connected to the door using concealed flexible wiring.

3.28.11 Single leaf doors (solid frame)

The Contractor shall provide an electric mortice lock / electric strike connected to the door using concealed flexible wiring.

3.28.12 Bi-parting doors

The Contractor shall provide motor lock hardware, input/output modules logic controller and interface to allow control of the doors by the access control system, and provide battery backup.

3.28.13 Cable transfers

Concealed cable transfers shall be used for each door fitted with electric mortice lock. Cable transfers shall be Abloy Style concealed transfers.

3.28.14 Door furniture

Regardless of the type of door furniture for other doors, all doors fitted with electric mortice locks shall be fitted with Lockwood 1800 series door furniture.

3.28.15 Lift controllers

All new and /or refurbished lifts shall have electronic access control.

The Contractor shall provide a Low Level Interface between the Lift system and the Siemens SiPass Integrated System. If this cannot be provided, notify the Security Manager.

The Low-level Interface shall include the use of a Siemens OPM multipurpose input/output module.

The Contractor shall supply and install access control to lifts as detailed. Where contactless card readers are required to be installed inside or outside the lift, the card reader shall be located on the lift control panel. Liaise with the Lift Contractor for the provision of lift trailing cable requirements.

3.28.16 Fire alarm interface

An interface to the building fire alarm systems is necessary to notify security of a fire alarm within the building and initiate the unlocking of all electric locks in the event of a fire alarm. This interface must be made to all connected fire systems including sprinkler and Fire Indicator Panels.

All lock power supplies shall pass through a relay contact, which shall be controlled by the fire system/s and shall be the two-pole type. The second pole shall be used to monitor the state of the fire relay and shall be programmed to activate an alarm input on the Command Centre.

3.28.17 Fire exit / emergency exit doors and alarms

Where exit doors form part of a required emergency egress path of controlled facilities (multimedia/library and the like), the Contractor shall provide an alarm that operates on door opening. These doors shall be provided with a local and/or remote audible alarm, as appropriate to alert staff of a breach of security. Visual alarm indication only required as necessary. Confirm these requirements with the University of Adelaide Security Manager.

All doors classified as Fire Doors or Emergency Exit Doors are to be configured in the following way:

- On an activation of the Fire Alarm Panel (FIP) a signal is to be transmitted to the Security Monitoring System (SMS) and all fire and emergency exit doors are to be electronically released, to allow free egress from the building
- An emergency release glass break unit is to provided adjacent each Fire Exit or Emergency Exit Door located in a prominent position on the lock side of the door. The glass break unit when activated is to remove power from the door-locking device.
- Locking devices shall be configured for fail-safe operation.

3.28.18 Access for the physically challenged

Unless otherwise specified, special provisions shall apply to all reader controlled access doors to improve accessibility for the physically challenged.

3.29 Door contacts

3.29.1 Magnetic reed switches

The Contractor shall provide magnetic reed switches which operate when:

- A personnel door is opened > 20 mm at the lock/latch edge
- The fixed leaf of a double door is opened > 20 mm at the lock/latch edge
- A vehicular door is opened > 100 mm

3.29.2 Construction

The Contractor shall provide concealed type magnetic reed switches for pedestrian access doors, and heavy duty roller door type magnetic reed switches for larger equipment access doors and roller doors.

3.29.3 Door monitoring (reed switch)

All Door Monitoring reed switches shall be GE Sentrol 1078 Series (19 mm or 25mm) hermetically sealed magnetic reed switch, or approved equivalent.

Surface mounted reed switches may be used where flush mount is not suitable. Approval is required from the University of Adelaide's Security Manager.

3.30 Vehicle control

3.30.1 General

The Contractor shall provide a vehicle access control system combining connection to vehicular access doors, boom-gates and interconnection to the main access control system.

3.30.2 Push-buttons and readers

The Contractor shall provide direct wall mounting for push-buttons or readers; otherwise provide a mounting bollard and extension arm.

3.30.3 Monitoring

The Contractor shall provide heavy duty reed switches on both inside extremities of vehicle doors, which generate a door closed indication at the control panel.

3.30.4 Exit loops

The Contractor shall provide exit loops as indicated on the drawings.

3.30.5 Boom-gates

The boom-gates shall be controlled via data readers and remote release. Provide boom-gates at the locations indicated on the drawings.

3.30.6 Roller shutters

Interface to all electrically operated roller shutters as required providing the Security service required. Provide separate UP/DOWN controls for each roller shutter.

3.30.7 Vehicle exit pedestrian warning

The Contractor shall provide vehicle exit pedestrian warning devices at locations shown on the drawings.

3.31 Intruder detection system

3.31.1 General requirements

Intruder detection devices shall be connected to the access control system as individual alarm 'points'. The intruder detection system shall provide the following minimum requirements:

- Provide full supervision of network cabling;
- Support monitored alarm circuits;
- Provide 24 hour supervised alarm zones (programmable).

The Contractor shall provide a Siemens SiPass Integrated electronic security solution. The SiPass Integrated system shall include but not limited to:

- SiPass Integrated Server;
- ACC5100 - Advanced Central Controller (ACC)
- AFI5100 - Input Point Module (IPM)
- AFO5100 - Output Point Module (OPM)
- AFO5200 - Multipurpose Input/output Module
- Power Supply Unit (PSU).

The Contractor must provide to the Security Manager Shop Drawings showing the proposed panel layout and panel locations. Approval must be granted before commencing work. Any deviation from this shop drawing as part of a project requires consultation and formal agreement of University of Adelaide Security Manager.

3.31.2 Alarm control panel

The Alarm Control Panel shall be a Siemens SiPass Integrated Advanced Central Controller, or approved equivalent.

The SiPass Integrated Server shall communicate with Advanced Central Controllers via Ethernet using TCP/IP communications.

The Advanced Central Controller communicates with local field devices, as listed above using RS-485 communications.

3.32 Anti-tamper devices

The Contractor shall provide anti-tamper devices to panels, detectors, control and activating devices, and access control devices.

3.32.1 Alarm circuit supervision

At each detection device, the Contractor shall provide four-state alarm circuit supervision using an end-of-line device connected via a separate circuit within the cable.

3.32.2 Configuration

The Contractor shall liaise with the Security Manager for confirmation and approval of the IDS and EACS system configurations including but not limited to:

- Areas and zones settings
- Arm/disarm requirements
- Entry/Exit delays.

3.32.3 Audible and visual alarms

The Contractor shall provide audible and visual alarms at locations shown on the drawings, which operate when an alarm condition exists.

The visual alarm shall reset automatically once the alarm condition is removed.

3.33 Movement detectors

3.33.1 Movement detectors - general

The volumetric detectors / devices shall comply with the following:

- Detect rapid changes of infra-red energy radiated within the detectors field of view
- Have an adjustable detection field
- Dual element
- Tamper alarms as separate output contact
- Have facilities to allow all cable entry and mounting holes to be sealed after installation to prevent ingress of insects etc.
- Be designed for wall or ceiling mounting as required by the drawings
- Removal of the lens cover shall result in the generation of a tamper condition
- Sufficient horizontal and vertical adjustment to allow coverage of the areas to be optimised.

Detectors shall be positioned to ensure that mounting height corresponds to the manufacturer's recommendations.

3.33.2 Passive infra-red motion sensors

All Passive Infra-Red Motion Sensors shall be as per Schedule 4.1 Equipment schedule.

3.33.3 Dual technology motion sensors

All Dual Technology Motion Sensors shall be as per Schedule 4.1 Equipment schedule.

3.34 Glass break detectors

The glass break detector shall be dual flex/audio detection separate microphone.

All Glass break detector shall be as per Schedule 4.1 Equipment schedule.

3.35 Remote arming station

The remote arming station shall be as per Schedule 4.1 Equipment schedule.

3.36 Intercommunication system

3.36.1 General requirements

All call points and intercommunications are managed by the University of Adelaide's ITS department.

All emergency call points shall have CCTV coverage.

3.36.2 Emergency call points

The Contractor shall refer to the UofA ITS specification for the manufacture, model, operation and interfacing.

3.36.3 Lift call points

The Contractor shall refer to the UoA ITS specification for the manufacture, model, operation and interfacing.

3.37 Closed Circuit Television (CCTV)

3.37.1 General requirements

The University of Adelaide ITS Department are responsible for the:

- CCTV VLAN
- Video Storage
- POE Switches
- Genetec Client Workstations
- Network design and bandwidth.

The contractor shall liaise with the Security Manager and the ITS Department before the installation of additional network camera(s).

3.37.2 Internal cameras

All internal cameras shall be as per the equipment schedule.

3.37.3 External cameras

All external cameras shall be as per the equipment schedule.

3.37.4 Video Management Software (VMS)

The server software shall be the latest Windows Server running Genetec Security Center video management software.

3.37.5 Recording and storage requirements

All storage requirements are managed by the UofA ITS Department. The Contractor shall coordinate with the UofA ITS Department to confirm storage requirements.

The internal and external cameras shall be configured, as a minimum for the following recording rates:

- 5 fps at 1080p, event triggered recording for Internal Cameras.
- 5 fps at 1080p, continuous recording for External Cameras.

3.38 Testing, commissioning & acceptance

3.38.1 Equipment and operation manuals

Provide manuals comprising plastic ring binder(s) with the project title, location, proprietor's name and contractor's name embossed on the covers. Pages not forming part of a multi-page brochure or technical manual are to be originals (i.e. not photocopies), and protected using plastic protectors designed for inclusion in the plastic ring binder. Incorporate the following information:

- Overall index for every inclusion in each of the volumes including drawings, technical brochures and the like
- Index for each volume which indexes every inclusion in that volume including drawings, technical brochures and the like
- A written text in the form of a system overview for each security services sub-system installed, and a detailed description of each sub-system's connectivity, location of lowest level equipment assemblies, technical operation and basic fault-finding steps
- Recommended maintenance periods and planned preventive maintenance procedures
- Copies of manufacturers' warranties or guarantees, service manuals, brochures, recommendations, etc.
- A copy of each work-as-executed drawing, cabling schedules, system configuration and programming schedules, equipment drawing, schematic drawing, and the like relevant to the installation
- A list of service companies and agencies for maintenance of components, equipment and systems in the installation
- A copy of all commissioning test results.

Simple references to manufacturers' handbooks or drawings are not acceptable.

3.38.2 Quantity

The Contractor shall provide quantity three of each volume of the Manual.

3.38.3 Submission

Submit a draft copy of each of the manuals for approval to the Security Manager, before submission of the final copies of the manuals. The draft manuals shall be submitted 14 days prior to Practical Completion.

3.38.4 As-installed drawings

The Contractor shall provide copies of the as-installed drawings as follows:

- A hard copy of each as-installed drawing in each equipment manual;
- A soft copy (on CD) of each as-installed drawing in each equipment manual; and
- An additional soft copy (on CD) of each as-installed drawing for retention by the Security Manager.

All as-installed drawings shall accurately reflect the installation in terms of equipment locations, mounting heights, cable and conduit routes (including pits and external conduits).

3.39 Operational instruction

3.39.1 Personal instruction

The Contractor shall provide personal operational instructions for each operator position to personnel nominated by the Security Manager.

3.39.2 Written instruction

The Contractor shall provide written operational instructions, matched to the training syllabus, for each operator position for all equipment. Include, with the written instructions, A4 schematic layouts showing the location and type of all the installed equipment through the building(s).

The written instruction shall form the basis of the Operator Manual. The training is to include system configuration, operation and routine maintenance.

3.39.3 Timing of instruction

The training session shall be provided prior to Practical Completion.

3.39.4 Length of instruction

The length of instruction shall be determined in conjunction with the Security Manager.

3.39.5 Notice

The Contractor shall provide 14 working days' notice of the proposed date for the instructions.

3.40 Acceptance testing

3.40.1 General

Inspections, document submissions and tests shall be carried out, including out-of-hours tests, to demonstrate compliance with the security services documentation, including all specifications, standards and referenced documents. The Acceptance Test Document, described below, forms the basis for confirming that compliance.

Equipment Test Sheets shall be provided as part of the Acceptance Test Document. These test sheets shall form a separate section which details each test procedure and each piece of equipment, including its unique serial number and drawing reference, to be subjected to that test procedure. Test results, for each test and for each piece of equipment, shall be recorded and are to include details of the actual measurements taken and not a general comment such as 'okay'.

This section shall also include, for each test and each piece of equipment, a specific area for entering a defect report number. These defect report numbers shall be cross-referenced to defect notices.

As part of the Acceptance Test Document there shall be a separate section for recording each defect report. The report shall contain the unique defect reference number, a cross-reference to the test procedure, equipment serial number, details of the defect, a corrective action area, a sign-off area for the technician and the contractor's supervisor and a witness sign-off area.

The acceptance test document shall be used for the Contractor's testing and commissioning. The completed document shall then be used as the basis for acceptance testing, and sign-off, prior to Practical Completion.

3.40.2 Equipment

The Contractor shall supply all necessary facilities, labour, apparatus and properly calibrated instruments required to test the installation, all of which shall be deemed to be included in the scope of work of this specification.

3.40.3 Test results

The Contractor shall provide typed and signed copies of commissioning and acceptance test/inspection schedule results, witnessed by the installation Supervisor.

3.40.4 Intruder detection

The Contractor shall undertake the walk testing of all movement detectors to ensure adequate coverage of the areas specified.

3.41 System monitoring

3.41.1 Commissioning

Except where the system is presently being monitored, the commissioning will proceed in two stages.

3.41.2 Stage 1 – pre commissioning

On completion of the installation and staff training, two days of system performance monitoring is to commence. This monitoring is to be undertaken on site. All costs are to be paid for by the Contractor. All faults associated with the installation including equipment failure, false alarms and insufficient staff training must be rectified during this stage.

3.41.3 Stage 2 - Final commissioning (to be done out of normal working hours)

The Contractor is to give a minimum of 5 days' written notice of the date of final commissioning. During this stage a full inspection including walk tests and voltage checks will be conducted. Disable the walk test facilities upon completion of the commissioning.

The Contractor is to provide the following at the time of commissioning:

- All manuals required as part of this specification; and
- Maintenance Log Book.

A defects list will be given to the Contractor following this inspection. Monitoring and response will continue to function as in Stage 1 (without cost to the Security Manager) until all defects have been rectified.

3.42 Separable portions

If a building is part of a Separable Portion and thus has an early Date of Practical Completion, ensure the security services for that building are fully operational at its Date of Practical Completion. If the permanent location of the 'control' equipment is not in the first Separable Portion to be handed over, make temporary arrangements so that the system can operate for the first handed over.

3.43 Practical completion

The Security Services shall be deemed to be ready for Practical Completion commissions and acceptance testing only when:

- All systems are fully operational;
- The Acceptance Test document has been submitted and approved;
- Completed test sheets forming part of the Acceptance Test document from the subcontractor(s) and witnessed by the installation supervisor as part of the installation QA procedure, have been submitted; and
- Completed test sheets forming part of the Acceptance Test document from the subcontractor(s) and witnessed by the installation supervisor as part of the installation QA procedure, for the 'specific tests' have been submitted.

3.44 Warranty

3.44.1 Scope

This section sets out the requirements for the provision of warranties.

Make good any defects caused by faulty workmanship and/or materials during the Defects Liability Period upon notice to do so.

3.44.2 Defects liability

The Contractor shall provide a minimum of a 12 month defects liability period from the date of acceptance by the University of Adelaide's Security Manager.

In the event of inclusion of equipment normally covered by a lesser time warranty, allow for and include the cost of extending such warranty to that specified for the whole installation.

3.44.3 Equipment warranties

Warrant the performance of all items of equipment used in the Works are not less than those specified when operating under the specified conditions and that such equipment can be installed with adequate clearances for operation and maintenance.

Replace any items of equipment not meeting the requirements, at no cost to the Security Manager.

Note: Replacement and/or repair of equipment during the Defects Liability Period may result in the Defects Liability Period being extended for that respective item/s.

3.44.4 Product application warranties

The systems offered shall be provided with the maximum Product Application Warranty that can be offered by the equipment manufacturers.

SCHEDULES

H. Security Services

4. SCHEDULES

4.1 Equipment schedule

Item type	Specification details
Electronic Security System	Siemens SiPass Integrated
	Advanced Central Controller (ACC)
	Input Point Module (IPM)
	Output Point Module (OPM)
	Single Reader Interface (SRI)
	Dual Reader Interface (DRI)
	Eight Reader Interface (ERI).
Card Reader	HID SE R10 Bluetooth Mini Mullion Reader
Key Pad	Siemens ATI5100 Arming Terminal
Electric Mortice Lock	Lockwood 3570 / 3582 Series
	Legge 990MFE
Electric Strike	Padde ES2000 / ES9000
	FSH FES20M
	Legge 8800M
Maglock	FSH 3500 / 5700 Series
Break Glass (call point)	Green 2 Pole, resettable
Egress Door Release	SOCA Infrared (touchless) Series
	32mm Green Mushroom, BT Products IR Switch Range (Not preferred- acceptable only in non-occupied spaces, e.g. store rooms)
Door Monitor Reed Switch	19mm Flush Mount
PIR Detector:	Optex or Paradox Range
Dual Technology	Optex or Paradox Range
Glass Break Detector	Optex or Paradox Range
Duress Call Point	Key resettable with controlled lock out process for reactivation.
Emergency Button	Red Mushroom Head Key resettable
CCTV Cameras	Axis Range

4.2 Preferred contractor contact details

Preferred contractor	Contact details
SiPass Integrator	BST Australia Security Systems &/or Consultants U3/ 482-486 South Road Kurralta Park, SA, 5037. Australia. Ph: (08) 8351 1877
Genetec Integrator	BST Australia Security Systems &/or Consultants U3/ 482-486 South Road Kurralta Park, SA, 5037. Australia. Ph: (08) 8351 1877