CSU GUIDELINES FOR CONTRACTORS INSTALLING GALLAGHER ACCESS CONTROL AND SECURITY SYSTEM

Gallagher Software Version 7.90

Updated – 07/01/2019
Please check you have the most current version of this document via the below URL

http://www.csu.edu.au/division/facilitiesm/tendering

Please note the following specifications detail equipment standards– final design must be authorised by the CSU Gallagher Custodian.

It is also to be noted that in 2011 Cardax had a name change to Gallagher; components of these products are one and the same.

SECTION 1

1.1 OVERVIEW
This document details requirements for the installation and configuration of Gallagher security & access control products on-site at the Charles Sturt University. The implementations of the processes within this document are to be applied and tailored specifically to each installation to meet the needs of the University.

1.2 SCOPE OF WORKS
This general specification will detail the performance requirements for the works that are to be carried out. This shall apply to the installation, supply or service of security and access control solutions to be delivered to the Charles Sturt University.

1.3 PROJECT REVIEW PROCESS
In the best interest of both the Charles Sturt University and the contractor it is a requirement that once final planning of scope and design of a security & access control solution has been defined it is submitted to the CSU Gallagher Custodian. A final review of the proposed design and the day-to-day functional operation of the planned installation will be carried out.
SECTION 2  ACCESS CONTROL SYSTEM

2.1 THE SYSTEM

This specification calls for the supply, installation and commissioning of extension and modifications to the existing Charles Sturt University ACIAS system currently installed in various buildings and facilities in NSW and ACT. All sections of the Charles Sturt University ACIAS are to be installed in accordance with appropriate local and international standards including BCA.

All access control doors must have forced door (FD) and door open too long (DOTL) alarms to help manage the various sites security. Break glass (BG) door releases will be required for electronically controlled egress doors where free handle egress door furniture is not installed. Request to Exit (REX) Buttons shall be used where fixed door furniture exists. The design for the Access system is to include monitoring of the emergency break glass units, forced door magnetic reed door contacts, electronic or electromagnetic locks, and electric strikes.

Access controlled doors will remain unlocked for an adjustable period (initially set at 5 seconds) on presentation of an authorised card or activation of a REX Button. On expiry of the selected time, doors must re-lock. A DOTL Warning will sound after 20 seconds and a DOTL alarm will report to Gallagher after 40 seconds.

The system shall monitor the condition of inputs. The system shall be able to be programmed to apply a variety of conditions to the way in which these inputs are monitored and how they enunciate the condition of the inputs. All inputs must connect to an individual alarm input, the only exception is a set of double doors, where each leaf is to be monitored in series as one input. Inputs shall be in a Closed Status in their Normal condition, 'input is inverted' shall only be used to ensure correct door operation when REX buttons are installed.

All hardware supplied will be of modern aesthetic design. Where flush mount or streamlined equivalents of devices are available that maintain full functionality they will be determined suitable for installation.

2.2 SERVICES INTEGRATION

The successful tenderer will be required to adopt and develop the universities vision for centralised security management. In order to satisfy the requirements of this vision, provision will be made for building systems to be integrated into the Gallagher system.

BMS/DALI INTEGRATIONS

All new security installations will require provision for low level relay control and monitoring of Building Management Systems and Dali Lighting systems. The contractor will liaise with the site electrician to arrange the required system connections.

This will include the monitoring of any cool room through the use of inputs into the Gallagher controller that will be programmed to trigger an alarm on the campus security phone on the alarm trigger.

Outputs will be programmed to trigger relays to allow for Gallagher operation of Dali Lighting systems throughout the proposed installation.

BUILDING SURVEILLANCE INTEGRATION

Where a security surveillance suite is used in any new project there will be requirement for the system to be integrated with the Gallagher Command Centre software. It is a requirement that all installed cameras will be indicated and accessible from Gallagher site plans. These integrations will include authentication to ensure that only authorised persons have access to view the cameras. The tenderer will refer to the Charles Sturt University CCTV Specification for details on CCTV integration requirements.
SYLLABUS PLUS INTEGRATION
Provision will be made for all future installations to involve configuration of the system integration for the scheduling of access control doors to be controlled by the Gallagher Syllabus Plus integration.

2.3 ACIAS PC

The existing Gallagher Server shall control the ACIAS at all remote sites. There shall be no additional head end located at any remote site. All software required for the works is to be supplied by the contractor and shall be in the name of Charles Sturt University. The existing server shall have site plans installed by the successful contractor with each device represented by an icon at the CSU server. The Site Plans shall contain hyperlinks creating a hierarchy of interlinked site plans. The Site Plans shall be imported from CAD drawings of the site prepared by the successful contractor, to the satisfaction of the CSU Gallagher Custodian.

2.4 CONTROLLERS

The Gallagher 6000 High Spec Controller, with 8H plug in module shall be installed in Communications rooms as indicated on the drawings.

All Gallagher equipment is to be installed in Gallagher Dual cabinets with Gallagher power supplies. Fire Trip compatible fuse cards shall be installed, with enough capacity for each powered lock relay to be individually fused. The Fire Trip card shall be monitored by a Gallagher input/s. All cabinets installed shall be complete with a lockable door, Gallagher master key compatible and must have a tamper alarm enabled.

2.5 SPARE CAPACITY

The successful tenderer shall allow 10% for future additional doors to be added. This 10% spare capacity is to include power, ports, inputs and physical space.

2.6 OPERATING VOLTAGE

All controllers are to be powered by a 240VAC GPO supplied by the CSU adjacent the controller. Provide any additional 240 volt AC mains power supplies to the system controllers and other devices as required for the works. Label all 240 volt AC mains power supplies. Where the Supply Authority requires inspection of equipment or the installation, the Contractor shall arrange for this inspection and payment of associated charges.

The provision of all low voltage power to all cabinets, racks, monitors, switches, computers etc., is the responsibility of the successful contractor.

This includes all cabling, conduit, wiring, terminal blocks, fuses etc., and any other items that may be necessary for the operation of the equipment.

The minimum size of cables shall be 2.5 mm2 (7/0.67) for 240 Volt circuits and 1.0 mm2 (7/0.40) for ELV power circuits. Due consideration shall be paid to voltage drop when calculating cable sizes.

The supply circuit breaker shall be labelled "ACCESS SYSTEM - DO NOT SWITCH OFF" by the successful tenderer.

All GPO's that support the Access Control/Surveillance systems must be contained either within a secure communications room or within a locked cabinet. These GPO's must not be directly accessible by unauthorised persons under any circumstances.
2.7 BATTERIES

All field equipment powered from the AC Mains supply shall incorporate a dedicated connection of ONLY re-chargeable Sealed Lead Acid batteries of 7.5 AH capacity to provide backup power in the event of Mains supply failure. Provide 12 Volt DC battery back-up with minimum capacity of 8 hours. Any batteries required shall consist of maintenance free sealed lead acid cells. (The date shall be written on the exterior of the battery with a permanent marker).

The equipment shall provide a suitable circuit to charge the batteries during normal operation. From flat the batteries will need to recharge to full capacity within 24 hours. The system shall be set up to monitor mains failure and low battery.

2.8 POWER SUPPLIES

The locks associated with the access control system shall be supplied from the Gallagher dual cabinet where the lock relay exists, the power supply must provide minimum 12 Volt DC battery back-up with minimum capacity of 8 hours. Instances where the Gallagher Dual cabinet with 8 Amp power supply will not will not meet this time period, additional Gallagher dual cabinets with 8 Amp power supply will need to be installed. If power supply exceeds 7.5 Amps, Additional Gallagher Dual Cabinets with 8 Amp power supplies will be required. These cabinets must be labelled to show they are power supplies only and which relays they are providing power to, in this instance notes shall be placed against affected devices in Gallagher programming.

All cabinets installed shall be complete with a lockable door, Gallagher master key compatible and must have a tamper alarm enabled.

The power supplies shall be connected to the base building Fire Indicator Panel (FIP) via the fuse card. The successful security contractor must Liaise with the fire contractor and pay all costs associated with the connection to the FIP, including any testing.

On activation of the building fire alarm the fuse card is to trigger and the ability to remove power from individual doors shall be achievable through this device. Any FIP which has the ability to affect a Gallagher access control door must be monitored by the Gallagher system as an input.

The Fuse Card/Fire Trip, Battery Low/Fail and Mains Fail shall be monitored individually by the ACIAS.

2.9 PHYSICAL ENCLOSURE PARAMETERS

All equipment enclosures shall be steel fabricated and powder coated. All field equipment shall be fitted with cabinet tamper detection capable of detecting any attempt to remove the cover and any attempt to remove the enclosure from its mounting surface. Tamper switches are to be monitored.

All Gallagher equipment shall be installed in Gallagher dual cabinets complete with a Gallagher 8 Amp power supply, lockable door, and must be Gallagher master key compatible. Each Cabinet must have a tamper alarm enabled. No cable entry shall be achieved through the underside of a Gallagher dual cabinet. A minimum of 2x 7 Amp batteries must be installed per power supply. The sticker provided by Gallagher for every cabinet, controller and expander must be filled out neatly, in pencil and be identical to the completed and approved programming names in the head end. The sticker must be neatly fixed to the inside of the cabinet door.

A cabinet lock shall be supplied by the Contractor for all new cabinets at each location. These must be keyed consistent with Gallagher cabinet locks.

2.10 KEYPAD CONTROL
The ACIAS system shall have multi-tenancy capacity for the monitoring and operation of different areas independently. This shall be achieved by using a T20 Multi Tech Terminal, Black in colour at the main staff entry door.

The system shall be capable of being used in a multitude of environments with all aspects of operation and programming being fully customisable to suit the needs of the client.

Standard height of keypads will be 1500mm to allow best visibility of the LCD panel.

2.11 ALARM OUTPUTS

Internal and external audio visual alarm units are to be installed both externally and internally to the site. External audio alarms are to reset after 8 minutes. Internal audio visual alarm units shall continue to operate until the alarm is reset. External visual alarm units are to include a flashing blue strobe light.

2.12 ALARM INPUTS

Four-state monitoring shall be used on all alarm inputs. A short or open circuit on the input shall force the Main Control Panel to activate a tamper alarm for that input and report the fault to the server. Alarms generated from the ACIAS include, FD & DOTL alarms, Break Glass alarms, Intruder Detection alarms and tamper alarms, Mains Fail, Battery Low and communications failure. Inputs are to be installed as a Normally Closed device and shall present as Closed status in the software. The only Inverted inputs shall be REX buttons.

All End of Line Resistors shall be encapsulated within the devices and be 4K7/4K7

2.13 NETWORK COMMUNICATIONS

All network cabling shall be installed in compliance with CSU DIT cabling standard. The current standard can be found at the below URL.

http://www.csu.edu.au/division/facilitiesm/tendering

CSU will provide the necessary switch port/s to allow connection to the CSU network. Any device connected to the CSU network will need to be DHCP compliant, written consent from the CSU Gallagher Custodian to install Non-DHCP compliant hardware must be obtained, before the installation of the hardware. The contractor must use a DHCP compliant version of hardware if one is available from the manufacturer.

The successful contractors shall liaise with and take direction from the CSU Networks Infrastructure personnel based in each Campus. All Network cabling patch leads installed for the ACIAS shall be Pink and labelled security.

2.14 SYSTEM PROGRAMMING

Programming is to be completed by competent, Gallagher certified, CSU approved Gallagher Operators, in their own name using their own Logon. Operator logons are provided to an individual person and are not to be shared or used by anyone other than the intended operator. Operators can be setup by approved DFM staff only.

Programming will include all requested access groups, individual doors including correct naming and function, time zones, alarm points, text and location names and site plans complete with icons etc. The ACIAS is to be supplied with all programming, equipment, hardware, software, cabling and ancillary services as required to provide a complete Access Control System and is to be functional in all respects.
All Programming includes the continuation of all CSU specific functions including but not limited to Action plans, icon assignment, Alarm instructions, SMS notifications and external door lockdown. Gallagher is programmed via individual Building Divisions, this should be completed in consultation with the CSU Gallagher Custodian.

Naming convention must be followed at all times, all devices attached to a door must have the same name as the door, with the addition of the ‘device programmed name’ (as below). Doors must have individual access zones named the same as the door, if a door requires two access zones, ‘Entry’ and ‘Exit’ shall be added to the door name for those access zones.

Naming convention will be obtained from CSU Web Site FM Central at the below URL.

For access control doors, the room number used will be the room being entered.

Below are two examples of the naming convention to be followed.

<table>
<thead>
<tr>
<th>Item Location</th>
<th>Campus ID (B,C,D,O,P,T, etc)</th>
<th>Building Code (4 digit)</th>
<th>Room Code (3 to 5 digit)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programmed Gallagher Name</td>
<td>Wagga</td>
<td>0253</td>
<td>Rm 103</td>
<td>Office Supervisor</td>
</tr>
<tr>
<td>Programmed Gallagher Name</td>
<td>Bathurst</td>
<td>1412</td>
<td>Rm 414</td>
<td>Tea Room</td>
</tr>
</tbody>
</table>

Devices shall be named as per the above naming convention, with the inclusion of the ‘Device Programmed name’ added to the end of the ‘Programmed Gallagher Name’.

<table>
<thead>
<tr>
<th>Physical Device</th>
<th>Device Programmed name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reed Switch</td>
<td>Reed</td>
</tr>
<tr>
<td>Lock Sense</td>
<td>LS</td>
</tr>
<tr>
<td>Tongue Sense</td>
<td>TS</td>
</tr>
<tr>
<td>Hub Monitor</td>
<td>Hub</td>
</tr>
<tr>
<td>Magnetic Lock Bond Sense</td>
<td>Bond</td>
</tr>
<tr>
<td>Request to Exit</td>
<td>REX</td>
</tr>
<tr>
<td>Break Glass</td>
<td>BG</td>
</tr>
<tr>
<td>Lock (output)</td>
<td>Lock</td>
</tr>
<tr>
<td>Door open too long</td>
<td>DOTL</td>
</tr>
<tr>
<td>Passive Infrared Detector 90</td>
<td>PIR</td>
</tr>
<tr>
<td>Passive Infrared Detector 360</td>
<td>PIR 360</td>
</tr>
<tr>
<td>Duress Button</td>
<td>Duress</td>
</tr>
<tr>
<td>Fridge Alarm</td>
<td>Fridge</td>
</tr>
<tr>
<td>Freezer Alarm</td>
<td>Freezer</td>
</tr>
<tr>
<td>Cool Room Alarm</td>
<td>Cool Room</td>
</tr>
<tr>
<td>Tamper</td>
<td>Tamper</td>
</tr>
<tr>
<td>Mains Fail</td>
<td>Mains Fail</td>
</tr>
<tr>
<td>Battery Low</td>
<td>Battery Low</td>
</tr>
<tr>
<td>Fuse Fail</td>
<td>Fuse Fail</td>
</tr>
<tr>
<td>Fire Panel, General Fire Alarm</td>
<td>Fire Panel Alarm</td>
</tr>
<tr>
<td>Fire Panel, Fault</td>
<td>Fire Panel Fault</td>
</tr>
<tr>
<td>Fire Panel, any active Isolation</td>
<td>Fire Panel Isolation Active</td>
</tr>
</tbody>
</table>
2.15 SOFTWARE

All software required for the works is to be supplied by the contractor and shall be in the name of the Charles Sturt University. Each door shall be provided with a license on a per door basis.

2.16 ACCESS TO STORED INFORMATION

User Authentication passwords shall be utilised and programmed by the successful tenderer to ensure only client authorised employees (i.e. Not contract security guards) can remove event records, passwords, user information and set up parameters. Any function that involves access to tools that allow the modification of system infrastructure hardware or software must be password protected. These passwords must reside with CSU.

2.17 SITE PLANS

On commissioning, Gallagher Site Plans will be completed for the project, these will be built on images produced from AutoCAD DWG files with all unnecessary Layers removed. Naming will be easily legible. Current Alarm Zone, Lockdown and Critical Power failure status will be clearly visible on the Site Plans. All Doors, PIR’s, Alarms, T20 Terminals and Cameras will be shown on the Site Plans.

2.18 CARD READER

Gallagher T11 Multi Tech Readers, Black in colour shall be installed, if a T11 (footprint 115mm x 70mm) will not physically fit, a T15 Multi Tech Reader, Black in colour can be used (footprint 139mm x 44mm). The final site positions of the individual readers shall be agreed with the CSU Campus services representative and sub-contractor, taking into account appearance, functionality and wiring access. All readers shall be mounted at the same height throughout the installation at a height complying with DDA and no more than 400mm from the door to be controlled.

Standard height will be level with the door handle or at 1100mm where no other reference is defined.

Card Readers shall not be mounted Back-to-Back on either sides of a wall, however shall be mounted offset at a distance to maintain integrity of card reader operation.

The Readers shall be installed in locations as directed by the CSU Campus services manager.

The Gallagher installer is also required to programme the CSU Mifare keys into all Gallagher Mifare readers prior to installation.

2.19 APERIO WIRELESS ACCESS CONTROL

The Gallagher integrated Aperio wireless door escutcheon is the prescribed product to be used on internal doors requiring a lock. The readers for these escutcheons are embedded in the escutcheon. The Aperio escutcheons are to be supplied and programmed by the successful tenderer in accordance with plans supplied and include the CSU Campus Services Manager’s requirements.

All Aperio hardware is to be purchased and installed via authorised Gallagher dealers and must include firmware installed by Gallagher. Standard Aperio hardware from any other source will not be accepted.

Aperio is not to be used for external doors or timetabled spaces.
Where Aperio Access Control Locks are to be used they shall be a Lockwood 3772 mechanical mortice lock. The escutcheon shall be version 3 AU103MU2SC1/1 and not have key override functionality.

2.20 SALTO WIRED (HOT SPOT) ACCESS READER

Where Salto system is required the Salto wired hotspot reader shall be installed externally to the main front entry of the building as directed by the CSU Campus services manager. This reader shall open the door on presentation of a valid, authorised card.

This shall be configured so the Salto Card operates the door via a Gallagher relay. The Salto controller must be connected to the Gallagher system via the Gallagher server which shall operate the door. Both the Salto and Gallagher server must be on the CSU VLAN Network.

Naming of the doors shall be as directed by the CSU Campus services manager.

2.21 SALTO OFFLINE ACCESS CONTROL – REMOTE AREAS ONLY

CSU integrates its Gallagher platform with the Salto offline Access Control system. These Salto readers are embedded in the door handle or padlocks with the reader configuration downloaded to the reader. The Salto readers are to be supplied and programmed by the successful tenderer as detailed on the plans supplied and are to be programmed in accordance with the CSU Campus Managers requirements. Salto is no longer used for mainstream buildings; it has been replaced by Aperio as the prescribed product for all internal doors requiring a lock. Salto can be used in remote areas where there is no data connection, IE farm gates, sheds ETC.

The Gallagher installer is required to program the CSU Mifare keys into all Gallagher Mifare readers prior to installation.

There will be no installation of Salto Offline access control doors on external doors due to maintaining live system auditing capabilities. The only exception being plant rooms with no through access.

Naming of the doors shall be as directed by the CSU Naming conventions via the Campus services manager.

2.22 CARDS

Cards supplied by CSU.

2.23 BREAK GLASS UNITS

Emergency break glass units shall be a Trojan Emergency Exit device mounted 900mm-1200mm above the floor on the side that faces a person seeking to exit. This unit shall remove power from the locking device and generate an alarm on the Access System. All break glass units shall be mounted at the same height throughout the installation of all buildings. All break glass units shall be monitored by the ACIAS and generate an alarm 24/7 if activated, if the break glass affects an access control door it must be programmed in the ‘emergency release’ section of the door programming. The break glass sounder must be connected for local audible function. The unit shall be installed in a manner which will allow the future installation of a Trojan Em Rex Cover, if required.

Emergency break glass units shall be installed in the locations detailed on the plans provided. The exact location shall be agreed with the architect, interior designer, sub-contractor and CSU, taking into account appearance, functionality and wiring access. Emergency break glass units
2.24 DOTL AND FD ALARMS

All access control doors will have forced door (FD) and door open too long (DOTL) alarms to help manage the site security.

All hardwired doors shall have an audio visual warning device located on the secure side, above the door, on the ceiling. This alarm shall be an Aritech AI 673 unit. In Residential locations, additional action plans will be required to email residential staff when this device or the reed switch associated with this device is tampered with.

The exact location shall be agreed with the architect, interior designer and sub-contractor, taking into account appearance, functionality and wiring access.

All access control doors will require a standard reed switch to achieve this functionality.

2.25 REX BUTTON

A Request to Exit (REX) Button shall be a Trojan Touch to Exit device. All REX buttons shall be mounted at the same height throughout the installation. This Device will be monitored as an input in the ACIAS only and shall not control the lock locally. REX inputs will need to be inverted through the software to work correctly when attached to doors.

REX Buttons shall be installed in the locations where fixed handles, magnetic locking or Auto doors are used. The exact location shall be agreed with the architect, interior designer and sub-contractor, taking into account appearance, functionality and wiring access.

All Free Handle doors shall have a rex input monitoring the free handle action.

2.26 DOOR HARDWARE

The CSU currently uses electronic mortise locks (Lockwood 3582ELMO or 3570ELMO) on most ACIAS doors. The successful contractor is to allow for all cut outs, core drilling and door transfer devices (LC8810 Cable Transfer) when installing electric mortise locks.

Electric strikes are NOT TO BE USED unless expressly requested via written documentation by the CSU Campus Manager. If used they shall be Padde ES2100 or ES9000 electric door strikes. These shall engage the door latch where used, without any backpressure on the latch hardware that will impede smooth operation of the door. Lock status and Tongue Sense monitoring must be utilised.

Wire to, install and commission each device. Provide concealed wiring with easily serviceable connections for all door locks, reed switches and audio visual warning devices. Where electric strike locks are used on entry only doors, a REX input shall be used to override the FD alarms, emergency exit will be by monitored break glass unit if no free handle egress is provided. Where entry and exit readers are used no push button is required. Where an egress reader is used, a monitored Break glass unit shall be used to exit in emergencies.

Where electro-magnetic door locks are used (Padde Z8) as advised by the CSU Campus Manager, and an exit reader is not used, the CSU specified REX shall be used to override the FD alarms and a fixed handle shall be installed, emergency exit will be by monitored break glass unit. Where an egress reader is used the ACIAS shall shunt the FD alarms and a monitored Break glass unit shall be used to exit in emergencies.

Doors are to have local sounding audio visual door forced (FD), door open too long (DOTL) and break glass monitoring (BG) units installed, alerting personnel of an alarm activation.

Where Aperio Access Control Locks are to be used they shall be a Lockwood 3772 mechanical mortice lock. The escutcheon shall be version 3 AU103MU2SC1/1 and not have key override functionality.

Where Salto Offline Access Control locks are specifically requested to be used they shall be Gainsborough 4400SS or Lockwood 3572 series.

<table>
<thead>
<tr>
<th>Door construction</th>
<th>Mortise lock</th>
<th>Gallagher Part No.</th>
<th>Salto Escutcheon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aluminium framed glass</td>
<td>Gainsborough 4400SS</td>
<td>C866206</td>
<td>E9450U00IM36-03</td>
</tr>
<tr>
<td>Wooden Door</td>
<td>Lockwood series 3572</td>
<td>C866203</td>
<td>A9650U00IM36-03</td>
</tr>
</tbody>
</table>

With wooden doors the contractor must determine the thickness of the door and therefore the length of the spindle prior to ordering the escutcheons from Gallagher.

The contractor is to identify CSU on the order so that the escutcheons are programmed with the CSU’s Mifare key at the factory.

Note: The Gallagher installer is also required to programme the CSU Mifare keys into all Gallagher Mifare readers prior to installation.

On framed glass doors, due to the narrow back set of the lock the handle can hit on the stop section of the door frame. The successful tender is to liaise with the builder and the door aluminium fabricator to allow for the Salto escutcheon to pass the stop section of the door frame.

Provide all plant, Labour and Materials to complete the works and co-ordinate and co-operate with all other trades associated with this trade work.

Note: Care should be taken to ensure that the selection and application of the locks on the doors meet the relevant BCA codes.

2.27 AUTO-DOORS

Where auto-doors are included on-site, strict requirements shall exist for the operation of these doors. The auto door options board shall be supplied by the auto-door installer to allow monitoring of the doors open position and Lock status at a minimum to the ACIAS.

Door control shall be achieved via two relays, the first is to change the door from Auto mode to secure mode. This relay will be programmed into the Door ‘Unlock Output’, ensuring the card readers display green when in ‘free’ access mode and red when in ‘secure’, it also enables operators to control auto doors in the same manner as other access control doors, without the need to locate a separate output/schedule. The second relay will ‘Drive the door open’ and will be required to trigger via a logic block when an authorised entry/exit action is performed for the door while in ‘secure’ mode.

During secure schedules entry will be obtained by an authorised card and not by any other means, exit will be by means of a Gallagher monitored Trojan REX push button or Gallagher
monitored Trojan break glass unit only. No non-Gallagher monitored door control will be accepted.

During periods of free access schedules, doors will be required to open via the auto-doors PIR detection for entry and exit.

Where the fire alarm is triggered or a break glass is activated the door will default to the always open position to allow free egress. In this state the DOTL alarm will be activated.

2.28 MAGNETIC REED SWITCHES

Magnetic reed door contacts shall be flush mount end on end reeds, of rugged construction and fitted to the leading edge of the door frame. Magnetic reed door contacts shall be installed on each leaf of double doors as a single monitored Gallagher input in series.

Magnetic reed switches shall be installed on all external perimeter doors for Monitoring Purposes.

A Roller shutter door contact shall be installed on the secure side of the roller door.

2.29 INTERCOM SYSTEM

The intercom system shall consist of a master control unit located at the reception desk with stations located at the front entry door, rear goods delivery roller door and rear door.

The intercom will allow the reception staff to talk to the person(s) waiting at the barriers for assistance. The reception will have the facility to open the barriers remotely from their station at the reception area.

The intercom master station shall be a telephone style handset and allow the operator to call and answer each station individually. The remote control of the doors shall only be programmed to work during business hours when the site is in access.

The intercom stations shall be constructed of an anti-vandal material and conducive to the architectural aesthetics of the building materials.

The system shall be loud enough at the remote stations to be clearly heard over any traffic noise. It is the intention and a requirement of this system that the reception staff be able to direct people to move on via the intercom system.

2.30 LIFT CONTROL

The final site positions of the individual readers within the lift cars shall be agreed with the architect, lift installer and sub-contractor, taking into account appearance, functionality and wiring access.

The Reader Interface Modules shall be installed in the security riser on the same floor as the lift motor room.

The Lift Module shall provide for “Normally Open” and “Normally Closed” Dry Relay Contacts to Enable/Disable Floor call buttons for each Lift Car to be controlled as detailed on the plans provided. These Relay Contacts shall be electrically isolated from the Access Control system.

Access rights associated with a presented CSU Card will be checked for validity based on access time and any other access management function defined in the system. Floor call button access shall be granted or denied, dependant on the access privilege programmed in Gallagher.
If the user does not have access to call the car, the car shall not move. The client will nominate the hours of operation of lift control. This may be 24/7 or after business hours only.

2.31 ELECTRONIC LOCKERS

All Electronic Locker Solutions installed at CSU, will be the Gallagher Locker Management solution, made available by Gallagher at version 7.9, final design of the solution must be approved by the CSU Gallagher Custodian.
3.1 SYSTEM DESIGN

The system will be designed in a format that all major traffic passages are monitored through the use of passive infra-red detectors. When triggered during armed periods these PIR’s will activate both a local alarm and a remote Gallagher system alarm and will trigger a notification to the Campus security phone.

3.2 VISUAL/AUDIBLE ALARMS

There will be provision for a visual indicator or strobe to be visible at all major building entries. There is also requirement for a local audible alarm to be triggered on activation.

3.3 DEVICE LOCATION

Passive infra-red detectors will be located at all major entries and throughout the facility. All high traffic areas and high risk areas must be monitored.

T20 terminals should be installed at major entry and exit points in highly visible locations, if possible in clear view of security cameras.

3.4 ALARM PROGRAMMING

During commissioning the alarms must be programmed with entry/exit delay that is tailored directly to the installation. All building entry and exits will be programmed to trigger entry delay.

Once the intruder alarm is triggered the system will be configured to send a notification message to the security phone and trigger a critical priority Gallagher Alarm.

CSU Campus Services manager will designate authorised individuals that will be given permissions to activate and deactivate the security alarm systems.

3.5 PASSIVE INFRA-RED / VOLUMETRIC DETECTORS

These detectors shall be Rokonet Iwise DT, Cosmos Quad Passive Infra-Red or Sentrol RCR-C or equivalent. 360 degree Volumetric Detectors shall be Aritech EV669 or Atsumi IR36E or IR110 or equivalent.

All End of Line Resistors shall be encapsulated within the devices and be 4K7/4K7.
SECTION 4 SYSTEM INSTALLATION

4.1 CABLE RETICULATION

All wiring shall be run inside the secure area of the premises with all cabling for the ACIAS concealed in ceiling spaces, wall cavities, equipment cabinets and field devices. All redundant wiring shall be removed.

Where this is not possible, install surface mounted conduits.

The tenderer shall survey the project site and take all notes and measurements necessary to provide a detailed and comprehensive understanding of the works specified.

All terminations for the ACIAS are to be within cabinets, enclosures, panels, detectors, housings, etc.

All network cabling installed in the patch rooms for the ACIAS shall be Cat 6e, pink and labelled security.

All cable penetrations must be fire stopped by the successful tenderer as required by local fire codes and ordinances. ACIAS System conduits and sleeves must be fire stopped by the successful tenderer using a UL-listed fire stop putty or fire rated blanket approved for such use.

Do not attach cables to ceiling hangers or any other service support. No cable, cable tray/ladder, cable duct or other horizontal cable component above the false ceiling shall be tied off to any light fixture, supports for any light fixture, electrical conduit, supports for any electrical conduit (Unistrut-Type structures excepted), sprinkler pipe, or any type of support for the sprinkler system.

Wire and cables shall be brought to the site in their original packages with their labels intact otherwise they shall be liable for rejection.

All wiring in which kinks or abrasions occur will be condemned and shall be replaced by the successful tenderer at the tenderers own expense.

Provide all wire and cable required to install systems as indicated. Wire and cable shall be sized to provide minimum voltage drop and minimum resistance to the devices being supplied. All cables shall be specifically designed for their intended use. Comply with equipment manufacturers’ recommendations for wire, fibre and cable. Colour codes shall be consistent in cables used for the same purpose. Comply with all applicable codes and ordinances; the insulation shall be to AS/NZS3000 as applicable.

Where joining of wiring cannot be avoided, wiring shall be joined using solder within panels, cabinets or field equipment. Jointing of cables external to a device will not be permitted.

Where wiring is to be run in the ceiling space it shall be neatly run in a regular manner and fixed at 1250mm intervals. Multiple runs shall be tied together along the common route at 500mm intervals and shall be either fixed to a cable tray or catenary. Cables shall not be left lying on the false ceiling. If more than 25 cables are in a single bundle, cable tray shall be used. Cables will be neat, tidy and run in order so it is possible to follow a single cable in a run over its entire length.

Due consideration shall be paid to voltage drop when calculating cable sizes.

All wiring shall comply with the latest issue of the requirements of the Local Supply Authority and AS/NZS3000 where relevant, any additional requirements specified hereunder, and the installation and cable route shall be to the satisfaction of the Project Manager.
The minimum size of cables shall be 2.5 mm\(^2\) (7/0.67) for 240 Volt circuits and 1.0 mm\(^2\) (7/0.40) for ELV power circuits. Due consideration shall be paid to voltage drop when calculating cable sizes.

**4.2 CONDUITS GENERAL**

Where cables can be concealed satisfactorily in ceiling spaces, and wall cavities, or they are run inside the secure area, conduits are not required. Where conduits are necessary, the following shall apply:

- Conduits shall be of minimum size 25 mm diameter, circular in section and shall be run so as to enable cables to be drawn-in after erection; sufficient accessible junction boxes shall be used for this purpose.
- Inspection fittings shall not be used for drawing in any cables.
- Where conduits are run on the surface on outside walls or exposed to the weather or are at risk of physical damage, the conduit shall be class ‘B’ galvanised steel screwed.
- Conduits shall be neatly run and securely fastened by means of approved saddles. All fixings, fastenings and supports shall be of adequate strength and arranged to ensure the installation against mechanical failure under normal conditions of use and wear and tear.
- Saddles shall be provided within 150 mm of all fittings or terminations.
- Rigid or flexible conduit drops shall be provided as required to provide connection to equipment.
- The direction of conduit runs shall be parallel to the walls, floors and ceilings, wherever practicable.
- The successful tenderer shall be responsible for the true horizontal or vertical installation of all boxes and fittings.
- Where junction boxes are exposed to the weather, the lids shall be sealed with an approved gasket.
- The boxes shall be of ample size to enable the cables to be neatly diverted from one conduit to another without undue cramping.
- Conduits shall be run concealed wherever possible.
- Surface conduits shall be run so as to be as inconspicuous as possible by running in corners, etc.
- The Project Manager shall approve the route of all surface conduits before installation is commenced.
- Exposed conduits shall be painted to match the surrounding surface. All exposed equipment that forms part of the system shall be painted to match the surrounding surface.

**4.3 STEEL CONDUIT**

Install steel conduit in areas where physical protection is required. Where steel conduits are necessary, the following shall apply:
• Steel conduit shall be manufactured in accordance with AS. 2052.
• All burrs shall be removed from ends and screwed bushes shall be fitted to the ends of conduit runs.
• 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.
• No threads shall be visible after erection other than running joints.
• Running threads shall be thoroughly painted with corrosion inhibiting paint prior to assembly.
• Pressed metal boxes shall be used for flush wall mounting equipment.
• Boxes shall have adjustable threaded fixing devices to permit flush mounting of the cover plate.

4.4 RIGID PVC CONDUIT

Where rigid PVC conduits are necessary, the following shall apply:
• Rigid PVC conduit and fittings shall be in accordance with AS. 2053.
• All joints shall be cemented with approved cement and fittings shall be of rigid PVC.
• Conduits and fittings damaged during installation or delivery will be condemned and shall be removed from site.
• Rigid PVC conduit shall be securely fastened with approved saddles spaced to prevent sagging.
• All sets and bends in rigid PVC conduit shall be made using internal springs of the correct size to prevent wall collapse, conduits in which any collapse of walls is evident will be condemned.

4.5 SECURITY CABLE TRAYS

The Project Manager shall approve the route and type of all cable trays before installation is commenced. Where more than 25 cables are run in a bunch cable tray shall be used not catenary wire. Catenary wire can be used for 25 cables or less.

Install cable trays as follows:
• All cable trays required for the ACIAS shall be neat and tidy.
• Cable trays shall be admiralty pattern, manufactured from hot dipped zinc plated sheet steel or cablofil wire mesh systems.
• The zinc coating shall be Z300 complying with AS1397.
• Steel sheet shall be a minimum of 1mm thick for 75mm wide trays, progressing to 2.5mm thick for 900mm wide trays.
• Edges shall have 90 degree folds of sufficient width to prevent sag and buckling between supports.

• Perforations in the cable tray shall be sized to accept expanding or clip type fasteners designed for the application.

• Fix cable trays using the unistrut system and provide the necessary clearance for installation of cables.

• Space fixing points at a maximum of 1200mm intervals.

Intervals shall be determined by the cable load capacity to prevent sag in all runs and be approved by the Project Manager.

4.6 LABELLING

Sample labels for all components of the ACIAS shall be provided for approval prior to installation.

Cable labelling schedules shall be prepared specifically for the project. All cables used for the ACIAS, shall be labelled at each end.

All labels will be machine printed using black text on a white background. Cable labels must use white self-laminating cable labels with black text.

All PC’s and monitors shall be labelled.

All Control Panels and Enclosures shall be labelled.

The 240V supply for the ACIAS shall be labelled “ACCESS SYSTEM - DO NOT SWITCH OFF” by the successful tenderer.

All access-controlled doors shall have appropriate signage and labels. All access doors shall be provided signage that reads “ACCESS CONTROLLED DOOR. DOOR IS NOT TO BE LEFT OPEN”.

All fire stair doors and fire exit doors with intruder detection systems installed shall be provided signage that reads “DOOR ALARMED 24 HOURS. EMERGENCY EXIT ONLY”.
SECTION 5 AS INSTALLED DRAWINGS & OPERATING MANUAL

On completion of the project, one (1) hard copy and one soft PDF copy of the following As Built documentation are to be supplied by the contractor.

As Built documentation is to be issued in a hardbound 4 ring white A4 folder clearly labelled-

ACIAS System
As Built Documentation
CSU XXXXXX
Security-In-Confidence

The As Built documentation shall include the following sections clearly separated with dividers for easy reference:-

- Table of contents.
- Contractor details, including 24 hour service contacts and 24 hour “Hot Line” Operational Support telephone contact number. Technical assistance program (TAP) numbers and 24 hour service contacts.
- Detailed Scope of works completed for the Security services.
- Bill of materials detailing product descriptions, equipment descriptions, part numbers and quantities.
- Bill of materials detailing product descriptions, part numbers and quantities in the form of an excel spread sheet.
- Product information.
- Schematic diagrams in CAD format.
- Full set of 1:100 scale as built drawings in hard and soft copy formats. The electronic drawings are to be in CAD format and must clearly indicate all equipment locations, outlet and device numbers and cable routes.
- Test results, Battery and monitoring test results.
- Controller, reader, Hub and Switch Layouts etc.
- System Schematic drawings
- Copy of customer training material.
- Walk test and commissioning information.
- Original software disks for all operating systems.
- A complete list of all software licences and registration details

The successful tenderer shall supply a complete electronic copy of all operating software following completion of installation and testing. The successful tenderer should note that provision of the above software constitutes part of the Commissioning process. Therefore, practical completion is also dependent upon provision of the above software.

At the completion of the defects liability period, the successful tenderer shall supply a completed updated electronic copy of all operating software.
SECTION 6 COMMISSIONING

6.1 ACCEPTANCE TEST PLAN (ATP)

The Security Contractor shall verify that the installed and commissioned system delivers the specified functionality and performance as a total system. The methodology shall be documented by the Security Contractor in an Acceptance Test Plan (ATP) and supplied 7 days prior to witness testing to the CSU Campus Services Manager and the consultant for sign off.

6.2 CHECKS UNDERTAKEN PRIOR TO WITNESS TESTING

Full commissioning checks must be undertaken prior to witness testing and final commissioning. All faults must be rectified at this time. Final commissioning actions and results must be fully documented. Results must form part of the As-Installed documentation.

The Charles Sturt University Commissioning Checklist will be referenced and completed during initial commissioning. All items will be checked as completed, on project handover the commissioning checklist will be signed by a representative of both the contractor and the Charles Sturt University.

Battery back-up tests and system monitoring and reporting confirmation, programming, system maps and setup and action texts must be proved at witness testing and actions and results must be fully documented. Results must form part of the As-Installed documentation.

A 14-day fault free period must be achieved after final commissioning and before practical completion of the works.

6.3 FINAL WITNESS TESTING AND COMMISSIONING

Utilising the completed walk test sheets, as installed documentation, battery test sheets and monitoring reports the system will be tested by the consultant and client in the presence of the account manager.

When defects or incomplete works are discovered during the witness test, a supplementary test at another date will be required by the University and as such the Contractor will be subject to full cost recovery.
Following final witness testing the consultant will issue a certificate of completion.
SECTION 7 MAINTENANCE

7.1 GENERAL

Provide twelve (12) months operational maintenance commencing from the date of practical completion and final acceptance of the commissioning tests for the complete ACIAS system. The site will be deemed to be operational once testing, training and monitoring begin and practical completion has been granted.

One (1) periodic maintenance visit is required during the first 6 months and the second visit 1 month before the expiration of the DLP period.

During the visit the Contractor shall complete and document the tests. Work required during periodic maintenance visits includes but is not limited to:

- All system maintenance checks are to be undertaken using the system password or master code.
- Check all 240 volt supplies feeding the system.
- Test all power supplies for full operation.
- Test the system on battery power and measure battery start and end voltages.
- Check reed switches, REX devices, locks, tamper switches, card readers etc.
- Check all PC's and monitors.
- Check that all panels and termination cabinet connections and contacts are free from corrosion and clean where necessary.
- Check wiring and conduits for tampering and damage.
- Test all devices and ensure that the circuit is sound throughout its entire length.

On completion of periodic maintenance, carry out short training refresher sessions for staff and the site security response staff as required.

The maintenance should include cleaning of all readers, door locks and electric strikes, code pads, MCP etc., inspections for loosened or corroded brackets, fixings, connections etc. and reprogramming of some functions of the ACIAS as required by the customer. Testing all alarm points back to the monitoring station and checking batteries.

Visits are to be carried out during normal office hours and in the presence of the nominated CSU Campus Services Authorised Person or staff member.

Specific dates for the periodic maintenance visits shall be nominated at hand over and the Contractor shall advise the CSU Campus Services Authorised Person 14 days in advance.

Appropriately qualified and licensed persons should conduct this maintenance. The system shall be inspected at least twice a year, or in accordance with the manufacturer’s recommendations and as nominated.

The tender shall provide a cost to maintain the complete ACIAS system for a period of 2 years, 3 years and 5 years with their response.

At the completion of each walk test, test sheets detailing the devices checked and their status must be supplied to the CSU Campus Services Authorised Person.

7.2 BREAK DOWN CALL OUT SERVICE

The Contractor shall maintain a 24 hour emergency service and advise CSU Campus Services of the emergency telephone number.

Whenever required by the circumstances or requested by the CSU Campus Services or Authorised Person, the Contractor’s Technician shall make phone contact with the requesting
CSU Campus Services or Authorised Person in relation to any repair, fault and or defect in the ACIAS within 1 hour.

Defects affecting perimeter security must be rectified within 1 hour of notification of a fault by the nominated representative.

Whenever required by the circumstances or requested by CSU Campus Services the Contractor’s Technician shall be on site to examine and repair any defect or reported fault in the ACIAS system within 4 hours.

If the repairs cannot be carried out within 24 hours, the CSU Campus Services Manager shall be notified.

On completion of a breakdown call out service the technician shall enter details of work performed to the CSU Campus Services Manager.

7.3 HOT LINE SUPPORT FACILITY

The Contractor shall provide a 24 hour “Hot Line” Operational Support telephone contact number to support CSU’s operational needs.

7.4 WORK OTHER THAN PERIODIC MAINTENANCE OR BREAK DOWN CALL OUT SERVICE

If and when so directed by the CSU Authorised Person, the Contractor shall effect alterations or repairs to any portion of the ACIAS systems, and shall promptly notify the CSU Authorised Person of any additional repairs necessary.

If work cannot be carried out within 24 hours, the CSU Authorised Person shall be notified in writing. The Contractor must obtain an Official Purchase number prior to undertaking any Work.

If outside normal working hours it is necessary for the protection of person or property that any repairs be effected urgently and there is no time to obtain the direction of the CSU Authorised Person then the Contractor shall carry out the necessary repairs and advise the CSU Authorised Person, and obtain an official CSU order number not later than the next working day thereafter.

Payment will not be made for repairs unless such repairs have been authorised in writing by the CSU Authorised Person.

An itemised account of all repairs including a full description of fault/action taken must be forwarded with any claims for payment.
SECTION 8 TRAINING

9.1 GENERAL

The Contractor shall provide a structured training and familiarisation program on the ACIAS for nominated staff. The Contractor shall make provision for two (2) separate sessions, each being a minimum of one (1) hours duration. The training sessions are to cover the following minimum requirements:

- Overview, function and operation of the ACIAS
- System alarm handling (turning on/off, acknowledging alarms).
- Operation of the system computer management software.
- Adding, deleting and changing user privileges.
- Adding, deleting and changing user codes.
- Generating reports.
- Interpretation of system generated messages and alarm responses.
- Viewing history logs.
- Isolating/de-isolating inputs and reports
- System integrity checks.
- Database management
- Programming / software maintenance
- Backing up of system configurations
- Event log archiving
- Understanding of Monitoring procedures and call out procedures.
- Guide through the user manual.
- General hardware architecture.
- Security standards for operators.
- Operator commands including online help functions.
- System diagnostics and fault finding.

As part of training requirements, the Contractor shall produce and distribute training material to each participant. They shall not be photo copies of manufacturer's brochures and catalogues except for illustration / component identification purposes. Training material shall be easily understood, system specific, logical and presented in a format consistent with approved training documentation standards.

Further, it shall be a requirement of the Contract for the Contractor to carry out short training refresher sessions during periodic maintenance visits.

The client shall advise the Contractor of the number of participants attending the training sessions.

The operator groups include

Administrators
Intermediate
Basic
SECTION 9  STANDARDS

The following standards are referenced in this specification and apply to this project:

The Building Code of Australia
Australia Communications Authority Technical Standards
AS/NZS 3000 SAA Wiring Rules
AS/NZS 1044 Limits of Electromagnetic Interference for Electrical Appliances
AS/NZS 1345 Identification of the Contents of Piping, Conduits and Ducts
AS/NZS 1367 Multiple Outlet Distribution Systems for Sound and Vision
AS/NZS 1768 Lightning Protection
AS/NZS 1939 Degrees of Protection Provided by Enclosures (IP Code)
AS/NZS 2052 Metallic Conduits and Fittings
AS/NZS 2053 Non Metallic Conduits and Fittings
AS/NZS 2201 Intruder Alarm Systems
AS/NZS 2279 Disturbances in Mains Supply Networks - Limitation of Harmonics
AS/NZS 2430 Classification of Hazardous Areas
AS/NZS 3147 Approval and Test Specification - PVC Insulated Electric Cables and Flexible Cables
AS/NZS 3159 Television Receiver Safety Requirements
All installed devices are to meet all required C tick Australian standards
Any other relevant standards ensuring quality, safety and system integrity.

Where any of the above applicable specifications, codes and standards conflict, the most stringent specification shall apply.

All works and services provided under this contract as a minimum must be in full compliance with the appropriate Australian Standard relevant to the works and services being carried out and provided by the contractor.

<table>
<thead>
<tr>
<th>Doc. Version Number</th>
<th>Date</th>
<th>Short description of amendment/s</th>
<th>Change Made By</th>
<th>Authorised By</th>
<th>To Match Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Nov 2009</td>
<td>Change of brand name from Cardax FT to Gallagher</td>
<td>Terry O'Meara</td>
<td>Terry O'Meara</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>17/08/2011</td>
<td>Change of brand name from Cardax FT to Gallagher</td>
<td>Terry O'Meara</td>
<td>Terry O'Meara</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>07/05/2013</td>
<td>Document Review</td>
<td>Adrian Wallace</td>
<td>Terry O'Meara</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>13/03/2014</td>
<td>Addition of Aperio</td>
<td>Terry O'Meara</td>
<td>Terry O'Meara</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>31/05/2017</td>
<td>Document Review</td>
<td>Tim Harris</td>
<td>Terry O'Meara</td>
<td>7.6</td>
</tr>
<tr>
<td>1.5</td>
<td>09/08/2017</td>
<td>Aperio clarification</td>
<td>Tim Harris</td>
<td>Terry O'Meara</td>
<td>7.6</td>
</tr>
<tr>
<td>1.6</td>
<td>21/06/2018</td>
<td>Document review and addition of Locker solution</td>
<td>Tim Harris</td>
<td>Terry O'Meara</td>
<td>7.8</td>
</tr>
<tr>
<td>7.9</td>
<td>04/01/2019</td>
<td>Document review, version numbering, name change and removal of contract terms and conditions to align with CSU website deployment.</td>
<td>Tim Harris</td>
<td>Terry O'Meara</td>
<td>7.9</td>
</tr>
<tr>
<td>7.91</td>
<td>07/01/2019</td>
<td>Inclusion of URL to obtain the up to date version of this document.</td>
<td>Tim Harris</td>
<td>Terry O'Meara</td>
<td>7.9</td>
</tr>
</tbody>
</table>