ACCESS CONTROL SYSTEM

REPLACEMENT

SPECIFICATION

FOR

THE HORNIMAN PUBLIC MUSEUM & PUBLIC PARK TRUST

Version 1_0

DOCUMENT INFORMATION

Project:	Access Control Upgrade Project
Client:	The Horniman Public Museum & Public Park Trust
Create Date:	14th November 2022
Your Ref:	
Our Ref:	20221011
Version No:	1_0

CHANGE HISTORY

Date	Version	Detail	Revised by	Reviewed by
14th November 2022	0_1	Initial Draft for Comment		TH
7th December 2022	1_0	Initial for Tender	WC	

CONFIDENTIALITY AND COPYRIGHT

DISCLAIMER

The information contained within the specification and supporting documentation is to the best of our knowledge true and accurate. Bridge Technical Consultants Ltd specifically exclude any liability for errors, omissions or otherwise arising there from.

All information, quantities and calculations should be verified by the Contractor as to its accuracy and suitability for the required purpose for use.

Contents

ABBREVIATIONS

ACS	Access Control System
AD	Active Directory
BTC	Bridge Technical Consultants Ltd
CCTV	Closed Circuit Television
CR	Control Room
GUI	Graphical User Interface
HMG	Horniman Museum & Gardens
ICT	Information Communication Technology
IDS	Intruder Detection System
IP	Internet Protocol
NTP	Network Time Protocol
NVR	Network Video Recorder
O&M	Operational and Maintenance
ONVIF	Open Network Video Interface Forum
OS	Operating System
PC	Personal Computer
PSU	Power Supply Unit
PTZ	Pan Tilt Zoom
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network

1. INTRODUCTION

The Horniman Museum & Gardens (HMG) is inviting tenders from suitably qualified and experienced organisations for the design, supply, installation and commissioning for the replacement of the existing Access Control System (ACS).

The Contract also includes the optional maintenance of the newly installed ACS for a minimum of one (1) year.

The security upgrade is to provide the Horniman Museum & Gardens with a like for like replacement of the existing ACS with no loss in performance and functionality, only improvements.

2. ASSOCIATED DOCUMENTS

2.1 Schedules

This document should be read in conjunction with the following schedules

- 20221011_Appendix 01 - Door Schedule

2.2 Drawings

This document should be read in conjunction with the following drawings

- 20221011_Appendix 02 - Nursery Cottage Plan
- 20221011_Appendix 03 - Bothy Gnd Floor Plan
- 20221011_Appendix 04 - Bothy 1st Floor Plan
- 20221011_Appendix 05 - Michael Horniman Building Gnd Floor Plan
- 20221011_Appendix 06 - Main Building Level 0_ Floor Plan
- 20221011_Appendix 07 - Main Building Level 1_ Floor Plan
- 20221011_Appendix 08 - Main Building Level 2_ Floor Plan
- 20221011_Appendix 09 - Main Building Level 3_ Floor Plan
- 20221011_Appendix 10 - Pavilion_ Floor Plan

The Contractor is to check all drawing notes as additional information may be recorded within an individual drawing to assist in the Contractors proposal and design.

2.3 Pricing Schedule

The pricing schedule is located in the following document: -

- 20221011_ACS_Replacement_Pricing Schedule

3. PROJECT INFORMATION

3.1 Project Overview

The ACS replacement project is to include the following: -

- Attend a virtual changeover process workshop to discuss and finalise how the ACS replacement is going to be conducted to minimise disruptions to HMG operations
- Install the new ACS server software within the HMG virtual environment
- Configure the new ACS servers software with the new ACS IP based single door controllers and any other required information
- Install the ACS workstation software so cardholder editing can be conducted ahead of the door controller hardware being changed over
- Install the ACS Active Directory (AD) software.
- Liaise with the HMG ICT department to link the new ACS and the HMG AD together so all staff cardholder information is passed between the two systems
- Provide the new ACS credentials so they can be issued to staff, volunteers and contractors before the ACS hardware is exchanged.
- Provide training on the new ACS so cardholder records can be added and edited
- HMG to update the ACS staff cardholder database with any information not imported by the HMG AD integration (Access Levels, credential card numbers, photograph, etc)
- HMG to add into the ACS cardholder database any required cardholder information that is not held within the AD, therefore not automatically populated into the ACS cardholder database.
- Conduct any required site surveys ahead of the changeover of the ACS controller and credential readers
- Exchange the currently installed ACS controllers and Credential readers across the museum in an agreed approach
- If selected for the project, install and commission the two (2) new control room doors into the ACS software
- If selected for the project, install and commission the new key cabinet and link to the ACS software
- Conduct further training as required
- Remove and return to HMG all redundant equipment that is no longer in use
- Provide a full set of updated O&M manuals

The list is not intended to be the complete list of tasks, or in the correct order that they are to be conducted, more detailed information of all the required tasks as part of the ACS replacement project are shown within this specification.

3.2 Project Parties

The employer for the ACS replacement project is: -

Name	Tim Hopkins
Job Description	Head of Estates
Email	thopkins@horniman.ac.uk

The technical consultant for the ACS replacement upgrade project is: -

Name	Warren Collins
Company	Bridge Technical Consultants Ltd
Email	wcollins@btc-global.com

3.3 Project Timeline

The anticipated project timelines are as follows: -

Task	Date
Tender issued to contractors	Friday 9th December 2022
Site visit day 1	Tuesday 20th December 2022
Site visit day 2	Thursday 5th January 2023
Contractor returns required by	Friday 13th January 2023
Tender evaluation and appointment of preferred bidder	Monday 16th January 2023 to Friday 27th January 2023
Start of installation of the ACS Replacement project	Monday 6th February 2023
Completion of installation of the ACS Replacement project	Friday 31st March 2023
Site acceptance & Witness Testing	W/C Monday 27th March 2023

The complete project MUST be completed by Friday 31st March 2023. Therefore it is imperative that the overall solution (software and hardware) proposed by the Contractor MUST be available for delivery, installation and commissioning before Friday 31st March 2023. The Contractor MUST NOT propose any products that cannot be delivered, installed and commissioning by Friday 31st March 2023.

As the credentials will be required to be distributed internally within the Museum ahead of the changeover of ACS hardware on the doors these credentials must also be available well ahead of Friday 31st March 2023 so not to delay the projects end date.

3.4 Site Location

The site location for the project are as follows: -

- 100 London Road, London , SE23 3PQ

3.5 Listed Status

The Horniman Museum and Gardens contains a Grade II* Listed building.

The Contractor must obtain permission from the HMG for any works that are to be completed that affect this listed building.

3.6 Site Visit

Contractors are invited to attend a site visit. The site visit dates are stated in the tender documentation. A maximum of two (2) representatives are invited from each company and their names are to be supplied in advance of the open day.

Contractors are to arrange a date with HMG at least three (3) working days before the site visit duration by sending the names of the representatives to the following

Name	Simon Mabbutt
Job Description	Security & Operations Manager
Email	smabbutt@horniman.ac.uk

The site visit day will allow the Contractors to visit the Museum. During the site visit Contractors can ask questions in relation to the project. All questions will be recorded and distributed to all tender companies. Any technical questions that cannot be answered during the open day are to be sent to the HMG procurement team for a response. Any questions relating to the upgrade project are bound by the dates as defined in the Project Timeline of this tender documentation.

It is the Contractors responsibly to fully understand this specification ahead of the site visit to ensure their visit provides all of the information the Contractor requires.

The Contractor is to ensure during their site visit the existing Power Supplies next to each of the Access Controlled doors are suitable for their chosen IP Based single door Controllers.

3.7 Project Plan / Gantt Chart

The Contractor is to provide a Gantt project plan as part of their proposal that includes the timescales and any dependencies on the tasks as defined in this specification. The project plan should contain any other tasks or dependencies the Contractor believes are relevant to the overall successful delivery of the project.

The project plan should be based on a project start date as stated in the project timeline of this tender documentation. The project plan should include any downtime the Contractor anticipates is required.

Along with the project plan the Contractor is to supply, as part of their return documentation, an explanation of their preferred methodology for the project, this must not exceed one thousand (1000) words.

3.8 COVID-19

The contractor is to comply with the Horniman Museum & Gardens policy.

3.9 Communication & Contact

No approach of any kind in connection with the ITT or the Procurement is to be made to any other person within or associated with HMG, or any other party. Failure to comply with this requirement may result in disqualification from the Procurement.

All communications in respect of the ITT or the procurement shall be in the English language.

3.10 Contractors Representative

The Contractor shall appoint a Contractor's Representative who is to act and make decisions on behalf of the Contractor for all purposes connected with this Contract.

The Contractor's Representative shall be contactable by phone during normal working hours to address any operational/other issues which may arise. The Contractor's Representative shall attend on site project meetings / witness testing as required.

The Contractor's Representative shall monitor contract performance and compliance with mandatory requirements on an ongoing basis.

3.11 Standards

All works shall be undertaken in accordance with the requirements of the following (but not limited to) where they are applicable: –

- BS EN 60839 Part 11-1. Alarm and Electronic Security Systems. Electronic Access Control Systems - Systems and Components Requirements.
- BS EN 60839 Part 11-2. Alarm and Electronic Security Systems. Electronic Access Control Systems - Application Guidelines.
- BS EN 62305-3:2011 Protection of structures against lightning - Physical damage to structures and life hazards.
- BS EN 62305-4:2011 Protection of structures against lightning - Electrical and electronic systems within structures.
- All relevant British Standards & Codes of Practice
- All relevant Building Regulations
- Construction (Design and Management) Regulations 2015
- Health & Safety at Work Act 1974
- Working at Height Regulations 2005
- Control of Substances Hazardous to Health (COSHH) Regulations 2002 (Latest Edition)
- The Waste Electrical and Electronic Equipment (WEEE) Regulations 2013
- Equality Act 2010

- Perform with reasonable care and skill in accordance with good industry practice using skilled and experienced personnel
- Not introduce any virus/vulnerability into HMG network or information systems
- Compliance with HMG regulations and standard provisions

3.12 CDM Regulations

The security upgrade project shall not be notifiable to the Health and Safety Executive under the Construction Design and Management Regulations (2015).

3.13 Discrepancies

Where an ambiguity may be discovered within the tender documentation the Contractor should seek clarification from the Employer.

Any assumptions or quantities taken without clarification by the Contractor are conducted entirely at the Contractor's own risk.

3.14 Induction

All Contractor staff are to attend a site induction before commencing any work on site.

3.15 Permits to Work

All tasks that are to be conducted as part of the security upgrade project will require permits to work. The Contractor is to allow sufficient time to obtain such permits as required prior to commencing any works on site.

3.16 Site Accommodation

The Contractor shall include within their proposal all of the costs required for any temporary site office and storage they require for the duration of the project.

The Contractor shall include for the secure storage of materials, tools, and equipment.

3.17 Contractor Manufacturer Certifications

The Contractors engineering team shall be currently certified in their proposed solution.

The Contractor is to provide training certificates from the manufacturer as part of their tender response.

At no time shall a Contractors staff member attend site to perform engineering tasks on a product on which they are not trained.

3.18 Contractor Certifications

The Contractor must be an approved company from one of the following organisations: -

- National Security Inspectorate (NSI)
- Security Systems and Alarms Inspection Board (SSAIB)

3.19 IP Based Single Door Controller - Approved Manufactures

HMG approved list of manufacturers for the upgrade project are as follows: -

Manufacturer	Product	Discipline
Axis	A1601 or A1001	IP Based Single Door Controller
Mercury Security	LP1501, LP1502 or LP4502	IP Based Single Door Controller

It is understood the above products are the only true open source non-proprietary IP based single door controllers that meet this specification.

When the above products are sold by ACS software manufacturers it is understood that the product names will be altered. However, the underlying product MUST be listed within this section of the specification.

No other products will be accepted apart from those listed within this section.

3.20 Compliance Statement

The Contactor is to provide as part of their tender submission confirmation that the proposal the Contractor is offering fully complies with this specification.

If the Contractor is unable to fully comply the Contractors proposal must detail all areas of this specification where their proposal cannot fully comply. The Contractor is to further detail how the proposal being offered differs from this specification.

If the Contractor fails to provide in their proposal a compliance statement, then the Contactors acknowledges their proposal fully complies with this specification.

3.21 GDPR / DPA 2018

While the ACS alone is not completely responsible for protection of data within it the ACS manufacturer and Contractor need to provide an overall solution that ensures the safety and security of the data held within the ACS.

Data retention policies need to be defined within the system and the system overwrites any data that is past this time period as well as alter the users to data that is being held past this period.

4. ACCESS CONTROL SYSTEM GENERAL REQUIREMENTS

4.1 Access Control System Software Functionality

The ACS shall have no numbered limitation as to its future expansion on either the access control of number of devices integrated.

The ACS shall offer a user-friendly environment with the user having control over alarm settings, report etc without Contractor support

4.2 ACS Help

The ACS shall provide a help software package that covers all areas of the ACS software.

The help should be available for all system administrators and system operators and have the following functions: -

- To be displayed via the F1 Function key or from Help on the ACS toolbar
- The Help is to allow searching via a keyword or search words
- Print the selected topic or the selected heading and all subtopics

4.3 Operator Privileges

The ACS shall have a username and password combination for each operator that accesses the system.

The ACS shall allow each operator shall be assigned an operator privilege level.

The ACS shall have no limit to the number of operators that can be defined within the system

The ACS shall have no limit to the amount of operator levels that can be defined within the system, such as card deactivation/activation only with no permissions to change access levels

The ACS shall not allow an operator access to any area of the ACS software that is not allowed within their operator privilege level

The ACS shall have an audit log that records any and all activity undertaken by the operator from time of login to logout.

The ACS shall allow for passwords to have a minimum-security strength to the set. This is to include special characters, length and complexity.

4.4 Cardholder Management

The ACS shall incorporate the ability to maintain cardholder data and the credentials each cardholder possess

The ACS shall support up to 10,000 cardholders

Features shall include the ability to:

- Add, Modify and Delete records based upon the operator's permissions.
- Capture photo images and signatures directly via a PC connect camera, Signature pad or import via picture e.g. JPG, BMP,etc
- Print cardholder information onto credentials.
- Search on any single database field.
- Customization of cardholder data fields
- The ability to assign multiple access levels to any cardholder
- The ability to assign a cardholder a PIN Number up to 8 digits in length.
- Support different types of cardholder e.g. Staff, Contractors, Visitors, etc
- The ability to make notes on each user's profile
- The ACS shall have an automatic credential deactivation function where a cardholder's credential will automatically deactivate after an extended period of inactivity based upon a predetermined time period. The credential status may be reset by authorized System Operators.

4.5 Cardholder Image Capture

The ACS shall be capable of capturing a cardholder's image from either a stored image file on the local PC or live video sources.

The cardholder image once captured shall be stored within the ACS MSSQL (or similar) database.

When capturing a cardholder image, the system operators shall be able to crop the image before saving into the ACS database and assigning to the cardholder.

4.6 Credential Print Designer

The ACS shall incorporate the ability to create and maintain card printing templates for single or dual sided print layouts.

Features shall include the ability to print on the credential the following: -

- Fixed text fields
- Database fields
- Cardholder images
- Fixed images

4.7 Credential Printing

The ACS shall support any printer with industry standard and Microsoft Certified Windows drivers.

Printers support shall include

- Retransfer
- Dye-Sublimation

4.8 Schedules

The ACS shall be capable of creating and storing an unlimited number of schedules for use in the ACS. A schedule is defined as a time period that can be applied to the ACS software.

The ACS shall support automatic adjustment for Daylight savings time

Schedules shall be used for the following: -

- Card Reader Functionality
- Access Levels
- Input Alarm Zones
- Output Control
- Event / Input / Output Linked Actions
- Cause and Effect responses

4.9 Access Levels

The ACS shall be capable of creating and storing an unlimited number of cardholder access levels for use in the ACS.

Each access level shall contain a list of all card readers and the schedules that are assigned to them to allow cardholders access.

The ACS shall support access levels where a cardholder can have multiple schedules set within the access level. The ACS shall not allow for only one access level to be assigned to a cardholder

4.10 Calendars

The ACS shall support a calendar whereby dates can be marked as holidays

The calendar can be applied to individual doors within the system thereby preventing access to unauthorised personnel during a holiday period e.g. Christmas Day

4.11 Card Formats

The ACS shall support multiple access control credential formats.

4.12 Door Configuration

The ACS shall support a limitless number of ACS doors.

The ACS shall allow the following to be set for every card reader on the ACS: -

- Scheduled Door Unlock
- Scheduled Keypad Only Entry
- Scheduled Reader and Keypad Entry
- Scheduled Reader or Keypad Entry
- Unlock Time
- Door Held Open Delay
- Extended Unlock for Equality Act Compliance
- Extended Door held open time for Equality Act Compliance

4.13 Door Alarms

The ACS shall allow each door to be configured to cause a variety of events to occur based upon activity at that door. The events may be caused by each of the following activities: -

- Door held open
- Door forced open
- Reject access attempt
- Break glass activated
- Fire door opened

The ACS shall allow alarms to be disabled for scheduled times and days of the week

4.14 Equality Act

The ACS shall support functionality that is fully compliant to the Equality Act

4.15 Inputs

The ACS shall support individual inputs to be defined within the ACS software.

The ACS shall support inputs groups to be defined within the ACS software.

The ACS shall allow the names of the alarm inputs to be clearly defined so making identification easy for operators

4.16 Outputs

The ACS shall support individual outputs to be defined within the ACS software.

The ACS shall support outputs groups to be defined within the ACS software.

The ACS shall allow the names of the alarm outputs to be clearly defined so making identification easy for operators

4.17 Event / Input / Output Linked Actions

The SMS shall support the ability for any Event or Input to be linked to any Event or Output which is available in the ACS system.

The linked actions shall be able to be time scheduled.

4.18 Reporting

The ACS shall include a reporter to display any ACS database information including configuration and event history.

The ACS reporter to contain the following functionality: -

- Standard reports to include (and not limited to) the following all with time and date stamped events
    - door opened
    - door forced
    - open too long
    - invalid card
    - valid card
    - system faults
    - alarm input
    - Cardholder database
- Search between two date time stamps
- Search on event time
- Export to file (TXT, Word, Excel, PDF)
- Export to Comma Delimited file (CSV)
- Export to SQL File (SQL)
- Export to database interface (ODBC, SQL,etc)
- Email to Recipient

4.19 Active Directory Integration

The ACS shall include LDAP integration.

The LDAP Integration shall: -

- Synchronize with an Active Directory domain within HMG
- Automatically Synchronize Active Directory users into the ACS Cardholder database
- Automatically Synchronize Active Directory data held for individuals into the ACS database
- Synchronize Active Directory cardholder images into the ACS database from the Active Directory
- Synchronize Active Directory cardholder images from the ACS database into the Active Directory
- Automatically assign basic access right to any imported cardholder from the Active Directory into the ACS database
- Remove cardholder access rights in the ACS based on their Active Directory status e.g. block a cardholder in the ACS is blocked in Active Directory

4.20 Interactive Plans

The ACS shall support the use of Interactive plans.

The Plans shall allow for multiple trees' to be built up which allows the linking of maps together.

There shall be no limited to the number of plans that can be used in the ACS.

The Plans shall allow the following to be placed on them: -

- Door Readers
- Inputs
- Outputs
- Command Buttons that can be set to perform configurable system actions e.g. print a report containing personnel who are on site.
- Network based ACS Hardware for status monitoring

The ACS shall support all current map file formats

The ACS interactive plans shall allow the System Operators to interact with the Icons placed on the plans, for example Lock, Unlock, Momentary, Lockdown and Lockdown Clear for a door.

The ACS Plans shall automatically present the relevant plan for a device should an alarm occur.

4.21 System Status Window

The ACS shall have a system status window which provides the ability to display the status of the ACS system.

The ACS shall support the ability for additional systems status reports to be created.

The system status window shall include, but not be limited to: -

- Active Points
- Disabled Points
- Disarmed Alarm Zones
- Energized Outputs
- Unlocked Doors

4.22 Manual Control

The ACS shall provide the system user the option to manually control parts of the ACS.

The Manual Control interface should include the ability to control:

- Doors
    - Unlock
    - Lock
    - Lockdown
    - Momentary unlock

4.23 Alarm and Event Management

The ACS shall support an alarm and event window within the application

The ACS alarm and event window shall be able to report any ACS event, message or alarm

The ACS alarm and event window shall display any event, message or alarm within 1 second of it occurring

The ACS alarm and event window shall be accessed only by correct operator login and privilege level.

The ACS shall allow for the ability to assign event or alarm instruction text for any ACS system message. The event text shall be displayed next to the event or alarm in the alarm management window

The ACS shall allow for the ability to assign event sounds for any ACS system message

The ACS shall allow the system alarms to be displayed as below: -

- Display at one or more ACS workstations.
- Alarms shall have priorities and higher alarms are placed above lower alarms in the alarm window.
- The ACS Alarm window will be brought to the front of any other open programs should an alarm occur.

The ACS shall allow the system alarms to be configured as below: -

- The Alarm shall always have a note assigned to it.
- The Alarm can / cannot be acknowledged if in an alarm state.
- Alarms can be printed.
- Alarms can have a sound assigned to them.
- Alarms can display a predefined Instruction for the System Operators.
- The interactive plans will display the associate plan and Icon.
- Acknowledge the selected alarm or acknowledge all alarms.

4.24 Fire Alarm Roll Call Reporting

The ACS shall provide fire alarm reporting when upon a fire alarm input that is activated on any ACS door controller will report as an alarm into the ACS alarm window.

Furthermore a report shall generated of those cardholder who have used their credentials that day in an individual building.

The report is then to be displayed on a monitor and automatically sent to a network connected printer.

The fire alarm reporting shall be based on individual buildings. As such each building will require a relay input from the local building fire alarm to be connected to a local ACS door controller. The Contactor is to investigate the individual building fire alarm relays during their site survey

4.25 CCTV Integration

The ACS shall provide a method to integrate with a wide variety of digital CCTV recorders.

This integration shall allow any CCTV images, live and recorded, to be displayed to an operator if a door local to the camera generates an alarm event

The function is not required as part of the ACS replacement project but to ensure compatibility for the future

4.26 Penetration Testing

The ACS manufacturer shall carry out penetration testing of their software and hardware to ensure it remains secure from cyber threats.

5. ACCESS CONTROL SYSTEM SOFTWARE REQUIREMENTS

5.1 Server Virtual Environment

HMG will provide a Windows virtual environment for the ACS server

The Contractors proposed ACS server software must be supported within a virtual environment. The Contractor is to provide the required specification of the virtual environment.

5.2 Server Functionality

The ACS Server shall support Windows Server 2019 as a minimum

The ACS Server shall not require manual user intervention to start any applications after a reboot

The ACS server's software operations shall be controlled by windows services.

The ACS shall use a windows service as a communication module to communicate with all of the ACS hardware.

The ACS Communication Module shall fully monitor all network-based ACS hardware and report any lost communication into the ACS alarm management window.

The ACS Communication Module shall monitor lost communications to any network-based ACS device and upon restoring of communications transmit any configuration changes that have occurred while the communication to that device was down.

No synchronisation of data problems shall occur between the ACS server and network-based ACS hardware as a loss of any communications.

The ACS Server performance shall not be affected by the scaling of the ACS system installed at HMG

The ACS server software shall be licensed by a software license and not use a physical hardware licensing method.

The ACS server software shall be licensed to support all of the ACS hardware and functions as required by this project

The ACS server software licensing shall allow for expansion to cover additional sites and offer a simple model of licensing as additions are made to the ACS

5.3 Transaction Log Truncation

The ACS server shall have the ability to truncate any transaction log files from a previous date by allowing the configuring of a date within the ACS software e.g. thirty (30) days so no cardholder transaction data is held past the configured thirty (30) days

The ACS server shall allow for the truncated transaction data to be removed from the main database and stored for later retrieval and investigation

5.4 Database

The ACS database shall be SQL based e.g. MSSQL, etc

The ACS should store all its cardholder, configuration and logged data within the database

The ACS should have a data cleanse process that can be automated to clear events after a specified amount of time.

5.5 Backup

The ACS software shall provide for both manual and automatic backups of the ACS database.

The ACS automatic backups shall be able to be scheduled and saved to a location not on the master or reductant server.

HMG will also perform a scheduled backup of the MSSQL database in line with HMG policy.

5.6 Licensing

The ACS server shall be fully licensed for connected devices

5.7 Plugins

The ACS Server and workstations shall be configured with all of the required plugins to operate the ACS including all integrations.

5.8 Workstations

The ACS shall support an unlimited amount of ACS workstations

HMG will provide the workstations for the ACS replacement project. The ACS workstation shall be Microsoft Windows 10 at a minimum. The contractor is to provide as part of their proposal the required specification of the workstations for their chosen solution.

The ACS workstations software to access the ACS software functionality shall be an installed application which is accessible from the All-Programs list.

6. ACCESS CONTROL SYSTEM HARDWARE REQUIREMENTS

The ACS shall comprise of tried and trusted resilient units that are readily available without import or other delays and known for its longevity of operation.

6.1 Non-Proprietary Hardware

The ACS IP based single door controllers MUST be non-proprietary hardware.

Only ACS door controllers that are supported by a number of ACS software manufacturers will be accepted.

The ACS software manufacturers who also support using the same IP based single door controllers non-proprietary hardware as proposed by the Contractor MUST have sales and technical support staff within the United Kingdom.

The ACS software manufacturer MUST sell their software, along with the IP based single door controllers non-proprietary hardware to installers within the United Kingdom

The ACS doors shall be powered by the existing local Power Supply Units.

The ACS hardware architecture is to consist of individual door controllers at each of the ACS doors.

See section 3.19 of this specification for the approved IP based single door controllers.

6.2 IP Based Single Door Controller

The ACS shall support multiple single door IP area controllers with door interface

The IP single door controller shall allow for standard network tools to be used for diagnostics e.g. Telnet

The IP single door controller shall hold all cardholder and door configuration within its local database

The IP single door controller shall not require the ACS server to be online to make any local decision and the controller will continue to allow access to cardholder upon presentation of a valid access control credential to any connected reader on the controller

The IP single door controller shall contain a 30,000 offline event buffer

The IP single door controller shall contain all of the inputs and outputs required to support a door operation at the correct voltage and current ratings

The IP single door controller shall support two (2) OSDP card readers, Read In and Read Out, on separate channels so the direction of travel is recorded in the ACS software.

The IP single door controller shall also allow for the second card reader to support an additional door and allow the door control to then provide control over two (2) doors if not used as a single read in and read out door.

The IP single door controller shall have additional inputs that can be configured for door position, RTE, BGU, tamper, fire alarm input or power monitoring.

The IP single door controller shall complete any badge events within half a second (0.5s) while under maximum load

6.3 Existing Housings and Power Supplies

The ACS single door IP controllers shall be mounted in the existing metal housing located by each of the existing doors.

The Contractor shall ensure the new IP Based single door controllers can be installed within the existing housing along with a 7.0ah battery. This is to reduce any making good of the surrounding area.

The ACS power supply shall be via non-switched fuse spur local to each power supply.

The ACS power supply shall contain a local battery backup to power the ACS hardware and all door equipment for 4 hours and not require replacement until at least 3 years.

The ACS local lock and ACS hardware that controls the door shall all be powered from the same power supply.

The Contractor is to ensure the existing ACS power supply housing is properly secure by installing any missing lid fixing screws

Withing the pricing schedule there is a line item for the optional cost to replace a Power Supply and Housing should any be discovered on site as being faulty.

Withing the pricing schedule there is a line item to install a new 7.0 ah battery per existing housing

6.4 Fire Alarm Interfacing

The Contractor is to ensure that any current connected fire alarm interfaces that connects to an existing door is also reconnected to the new ACS door controller.

The incumbent fire alarm company is Trinity Fire & Security System.

6.5 Access Control Credential Readers

6.5.1 Functionality

The ACS readers shall have the ability to read any cardholder credential and visually by LED and audibly report the read status as controlled by the ACS

6.5.2 Type

The ACS readers shall be of the 13.56 MHz type e.g. iClass, Mifare DESFire EV2

125Khz MUST NOT be used

The ACS readers shall offer different form factors included keypad to provide Pin and duress codes.

HMG do not require any keypads readers are part of the ACS replacement project.

6.5.3 Protocol

The ACS readers shall offer secure communication protocols between the reader IP based single door controller.

Acceptable communication protocols are: -

- Open Supervised Device Protocol (OSDP)
- Secure RS485

Wiegand protocol MUST NOT be used

6.5.4 Form Factor

To minimize on the making good of any exposed surface the chosen Credential Readers should be slightly larger, if possible, than the existing readers so the new reader does not require any painting should its form factor be smaller than the existing.

Door 19, Staff Entrances, Credential Reader is located behind the intercom front panel and the replacement reader should also be hidden in the same location.

6.6 Access Control Credentials

6.6.1 Functionality

The ACS credentials Card Serial Number (CSN) shall not be used by any part of the ACS.

Only encoded badge numbers shall be acceptable that are stored within secure a secure sector within the ACS credential.

6.6.2 Type

The ACS credential shall be of the 13.56 MHz type e.g. iClass, MiFare DESFire EV2.

125KHZ MUST NOT be used

The ACS credential shall support multiple format factors e.g. Card, Clamshell, Microtag etc

The ACS credential shall offer a method of securing the encoded badge number so obtaining of duplicate cards is not possible e.g. iClass secure keys, Corporate 1000 etc. The Contractor is to detail their proposed solution within their design.

The ACS credential shall not be of a known type that has been 'hacked' or had the security compromised so the card number can be read through other means.

The ACS credential shall be either supplied blank or encoding on site or supplied with a badge number already encoded into the credential. The Contractor is to detail their proposed solution within their design.

The ACS credential badge format shall not be proprietary to one supplier.

The ACS credential shall be capable of supporting additional data that is to be held on secure application areas on the credential. E.g. Cashless Vending, follow me printing, wireless door handles, etc

6.7 Existing Door Peripherals

The contractor is to reuse all existing door hardware as follows: -

- Locking Mechanism
- Request to Exit Button (RTE)
- Break Glass Unit (BGU)

Where any of the existing door peripherals are found to be faulty these faults are to be reported to the employer

There are no door position contacts currently installed on any door at HMG

Withing the pricing schedule there are line items for the optional cost to replace each of the existing door peripheral should any be discovered on site as being faulty.

6.8 Door Position Contacts

There are no door position contacts currently installed on any door at HMG for the monitoring of the doors position.

6.9 Key cabinet

The key cabinet shall be a floor standing cabinet that can support up to one-hundred and eighty (180) separate keys.

The key cabinet shall allow for 24 / 7 access to the keys for authorised users only.

The key cabinet shall have a full audit trail of all users and key transactions. A report must be able to run at the end of each day and report which keys are not held within the key cabinet

The key cabinet shall be fully integrated into the new ACS software so only authorised ACS credentials can be used on an ACS credential reader that is installed on the front the key cabinet. Once a valid authorised credential is used on the reader the key cabinets door shall open and the user can only remove those keys they are authorised to take.

When a user returns the keys to the key cabinet the user shall place the creation on the reader on the key cabinet front panel and the key cabinets door shall open. The user shall then return the keys to the allocated space within the key cabinet and then close the front door.

The Contractor is to provide details of their proposed key cabinet as part of their proposal.

6.10 Warranty Period

The Contractor shall state in their proposal the warranty period of the ACS equipment proposed

6.11 Warranty Agreement

All associated software and hardware supplied as part of the ACS replacement shall have the warranty agreement held with the manufacturer in the name of the Horniman Museum and Gardens.

The warranty agreement shall not be registered in the name of the Contractor.

7. EXISTING ACCESS CONTROL SYSTEM

7.1 Overview

The current EACS system installed within the HMG estate is from the manufacturer Kantech, who are owned by Tyco Security Products, and is the EntraPass product line.

The EACS comprises of nineteen (19) controlled doors with approximately two hundred (200) cardholders in the Kantech EACS database.

The architecture of the EACS door controllers at HMG is a mix of the following: -

- Ethernet connected (IP network)
- RS485 data line connected direct to the Kantech EACS server
- RS485 data line connected direct to other door controllers.

Unfortunately, during a change of server hardware the current Kantech EACS database was lost. Therefore the EACS running at the HMG is actually operating in a standalone mode.

7.2 Dilapidation Survey & Report

The Contractor is to complete a site survey report before undertaking any works on the ACS.

The report is to include all the following: -

- Confirmation of a mains fuse spur being present at the door location. If the mains spur is not present this is reported to MHG to prevent any delays in the project.
- Confirmation of an Ethernet cable being present at the door location. If the cable is not present this is confirmed as being due to be installed as part of the project to prevent any delays.
- The Contactor is to investigate the individual building fire alarm relays to ensure each building has a fire alarm relay for interfacing with the ACS for the fire roll call reporting
- Report any other factors that could delay the project at any door locations.

The Contractor is to complete a dilapidation report of the existing main building ACS.

The report is to include any known faults with any of the existing door peripherals that would affect the operation of the new ACS.

Where any of the existing door peripherals are found to be faulty these faults are to be reported to the employer for the appropriate action to be taken in resolving the fault.

8. ACCESS CONTROL SYSTEM REPLACEMENT REQUIREMENTS

8.1 Workshop

8.1.1 Changeover Process Workshop

As part of the upgrade project the Contractor is to attend a changeover process workshop with the Employer to agree the process and expected downtime of any ACS connected doors.

The newly upgraded ACS system is to replace the existing system with no noticeable degradation in performance and functionality, only improvements.

It is important to minimise downtime of the systems. All downtime must be agreed with the Employer. The downtime is to be kept to the absolute minimum.

The Contractor is to provide in the tender submission their method statement of how they will minimise downtime and what downtime if any, they expect there to be during the course of the project.

8.2 Access Control Server Virtual Environment

HMG will provide a Windows virtual environment for the ACS server

The Contractor is to install the ACS server software within the Windows virtual environment.

HMG will provide a remote access for this to be carried out via a PC within the Museums network.

8.3 Access Control Workstations

The Contractor is to install the ACS workstation software on the following PC's:-

- Security Managers Office
- Reception
- Reception Back Office

8.4 Existing Card Printer

HMG currently uses a LDP Smartt 31 card printer.

The new ACS must be configured to use this existing card printer that is located in the security mangers office.

8.5 Cardholder Image Capture

HMG require a desktop camera that can be sued within the security office to capture personal images.

The captured photo image shall be stored within the ACS database so it can be printed on the cardholder credential as well as available within for exporting to the HMG AD system via the integration between the two systems.

8.6 Active Directory Integration

The Contractor is to conduct the following: -

- Install the ACS Active Directory (AD) software
- Consult with the HMG ICT department to link the new ACS and the HMG AD together so all staff cardholder information is passed between the two system.

8.7 Importing of non- staff cardholders

HMG is in the process of recording all of the non-staff members, who are therefore not stored in the Active Directory system, within an excel sheet.

Ideally the new ACS shall have the facility to import this excel data set into the cardholder database to assist in the issuing of the new credentials.

8.8 Individual Door Controller Exchange

Once all of the HMG cardholders have been added into the new ACS software (Via AD import or manual entry) and their new credentials have been issued to them each of the individual door controller can be exchanged.

The Contractor is to conduct the following: -

- Each of the individual door controller, are to be removed and a new IP Based single door controller installed as per the previously agreed approach to ensure Museum operations are not affected and the existing ACS still operates
- The new door controller is to be connected onto the HMG supplied and installed Ethernet cable
- The existing Credential readers shall be removed and the new Credential readers installed. If the cabling requires replacing then this shall have been installed previously or completed during this changeover
- The existing door peripherals are to be connected to the new IP based single door controller
- The Door Controller is to be powered by the existing Power Supply within the housing
- The ACS door shall be enabled within the ACS software and the configuration sent to the new IP based single door controller
- The ACS door shall be tested fully to ensure all of the peripherals operate as expected and any credentials that are presented to the credential readers are working as expected.

8.9 Fire Alarm Interfacing

The Contractor is to ensure that any previously connected fire alarm interfaces that connected to an existing door, therefore opening the doors locking mechanism in the event of a fire alarm activation, is also reconnected to the new ACS door controller.

8.10 Door 13 Alarm

The Contractor is to be aware that Door 13 has a simple door alarm connected to it that generates an audible alarm should the door be opened via the crash bar. If the door is opened using the credential reader the door alarm does not activate.

The Contractor is to reconnect this door alarm so it functions in the same way.

8.11 Key Cabinet

The Contractor is to provide an optional cost for a one-hundred and eighty (180) key cabinet.

The key cabinet is to be installed within the staff entrance lobby

Power and data has already been installed for the new key cabinet.

The new key cabinet must interface into the new ACS software with a dedicated ACS credential reader installed on the front of the key cabinet

8.12 Fire Alarm Roll Call Reporting

The Contractor is to provide fire alarm roll call reporting as part of the ACS replacement project.

The ACS software shall, upon receiving a fire alarm activation signal from a connected fire alarm relay, generate a fire alarm roll call report.

The fire alarm roll call report is to contain all of the cardholders who have used their credentials during that day to enter an ACS door to a building.

The fire alarm roll call report shall be automatically displayed on a monitor and send to a museum connected printer for automatic printing.

The fire alarm roll call report must be fully automatic with no human intervention required.

It is understood that as turnstyles are not in use the fire alarm roll call data produced will only be for cardholders who have used their credentials to enter one of the ACS doors to a building.

8.13 Control Room Doors

The Contractor is to provide an optional cost to secure the existing control room doors.

The current two (2) doors are controlled by a Glutz 18945 locking mechanism with a card reader inbuilt into the handle.

The required operation of the control room doors is to have the following installed: -

- IP based Single door controller with housing and power supply.
- Credential Reader in
- Credential Reader Out
- Interface to the existing Glutz locking mechanism. The Contractor is to provide details of how this will be carried out.
- Any required software licensing

If this option is selected HMG will provide the required Ethernet cable for connecting to the IP network.

8.14 Door Position Contacts

There are no door position contacts currently installed on any door at HMG for the monitoring of the doors position.

An optional cost for the installation of door contacts is to be included as part of the contractors proposal.

It is anticipated that the contractor may well be able to use spare cores in the existing cable to the existing door locking mechanism. However, a survey of each doors existing cabling has not be carried out to confirm this and this is for the Contractor to confirm before providing an optional cost.

8.15 Monitoring of Break Glass Units

The currently installed Break Glass Units are not monitored by the ACS.

An optional cost for the installation of monitored Break Glass Units is to be included as part of the contractors proposal. When activated the ACS software shall displayed an alarm message so the Break Glass Unit can be checked and reset as required

8.16 Single Standalone Door

The contractor is to provide an optional cost for a standalone door keypad and locking mechanism.

HMG will escort the Contractor to the door during the site visits.

The door is to allow free access during certain times and then require a code to be entered to unlock the door during other times.

The Contractor is to provide the following within the optional cost -

- Standalone keypad with unlock schedule inbuilt
- Locking mechanism to secure the door
- Power Supply
- Cabling
- Installation

7. ICT REQUIREMENTS

7.1. Local Area Network

The complete security network is on a VLAN separate from the main HMG network and shall remain in the same configuration operating as a separate VLAN.

7.2. Cyber Security

The Contractor must ensure the deployment of the overall ACS follows industry best practices with regards cyber security.

These are to include the following where possible depending on the overall final design and architecture of the deployed solution.

- Deployed using the manufacturers cyber hardening recommendations.
- Be Cyber Essentials certified
- Ensure devices are secure and free from tampering
- No visible access to any RJ45 sockets
- Password are updated and not left as default or empty
- Disable all auto discovery features
- All Servers, Clients and cameras software, firmware and operating systems are up to date

7.3. Pre-Programming of Equipment

The Contractor may pre-program any or all equipment with the relevant IP information prior to delivery on site to assist in the deployment phase of the project.

7.4. Network Switches

All networks switches will be provided by HMG

7.5. IP Addressing

The Contractor is to consult with the HMG ICT team to obtain the required IP addressing information of the new IP based single door controllers.

7.6. Anti-Virus Software

HMG will manage all Anti-Virus software

7.7. Remote Support Connection

The Contractor is to provide remote support where any first line support calls can be remotely conducted by the Contractor. The Contactor is to consult with HMG ICT department on their preferred approved method of remote connection.

7.8. Firmware / Software Updates

The Contractor is to supply all new hardware with the latest firmware and software as released by the manufacturer at the time of installation.

7.9. Network Time Protocol

The Contractor is to ensure all IP based equipment, if this is available as an option in the devices programming, is synced to the HMG NTP server

7.10. Cabling Requirements

7.10.1. Ethernet Cable

The contractor is not to provide any new Ethernet cabling as part of the ACS replacement project.

All new Ethernet cable connections from the associated network switches to each doors PSU will be installed by HMG.

The Ethernet cable will be left outside of the PSU with spare cable to allow the Contactor to relocate the cable inside the PSU when the door controller is exchanged.

The Contractor is not to leave any exposed Ethernet connection external to the PSU.

7.10.2. RJ45 Sockets

It is not anticipated any additional RJ45 sockets will be required for this project.

7.10.3. Patch Cables

The Contractor is to supply a new CAT6 network patch lead at door number 14.

Door 14 PSU's is located directly next to the network switch and so no additional cabling will be installed by HMG.

The patch lead is to be a certified premade patch lead. Patch leads made on site are not acceptable.

7.10.4. Labelling

The Contractor is to label all cabling connected into the PSU.

7.10.5. Containment

The Contractor is to reuse all of the existing containment that is currently being used for cabling or install new suitable containment as required.

Any works that involve the installation of new cabling that include the installation of new containment must be agreed before the works are carried out.

A survey must be completed by the Contractor ahead of the ACS door controller being replaced to ensure any works have been identified and agreed ahead of time

7.10.6. Existing Cable Use

The contractor is to ensure all existing cabling is suitable to be reused by the replacement ACS hardware for all connected devices

It is anticipated the existing credential reader cabling may require to be replace if the cable is not capable of supporting RS485 communications as required.

While the majority of the existing credential reader is surface run in plastic box trunking the Contractor need to be aware some cabling may be flushed into the surrounding wall.

7.10.7. Existing Cabling Removal

All existing redundant cabling is to be removed by the Contactor and disposed of once the ACS replacement project upgrade has been completed.

7.11. Fuse Spurs

It is not anticipated any additional fuse spurs will be required for this project.

7.12. Disposal of Equipment

The Contractor is to dispose of all cabling and other ACS related equipment using the Contractors own approved WEEE Contractor once it is decommissioned and removed.

The Contractor is to provide waste transfer notes for all equipment removed from site and disposed of.

8. INSTALLATION WORKS

8.1. Co-ordination of Installation Works

All site works shall be coordinated with the Employer to ensure that access to areas is pre-arranged with each department.

8.2. General Requirements

HMG requires the contractor to provide a Risk Assessment and Method Statement (RAMS) prior to the work starting on any site, this is to be agreed an advance with HMG.

HMG will:

- Ensure competent contractors are engaged to work on its behalf and this policy and the supporting documentation will be followed to ensure this happens.
- Provide all necessary information and instructions relating to the works, including any relevant standards and procedures with which the contractor may be expected to comply, and site risk assessments as required.
- Ensure that contractors do not use tools or equipment owned by HMG unless express written prior permission is given.
- Provide a system to ensure effective communication and cooperation in respect of all works involving contractors including the undertaking of risk assessments by the contractor in respect of the job-related risks and by HMG authorised officer in respect of the site hazards. The assessments must follow the risk management hierarchy of elimination, or reduction to the lowest level reasonably practicable by effective control measures, and the effective management of any remaining risks.

All contractors will.

- Provide appropriate personal protective equipment (PPE) commensurate with the risks on each site as identified by the risk assessments. It will be the contractor's responsibility to provide such PPE as may be necessary
- Plan and manage works effectively with regard to health, safety, and quality of work.
- No contractor/sub-contractor shall start work on site or deliver a service until such time as HMG is satisfied that all aspects of health and safety have been dealt with and the Health and Safety Officer must be notified when they will start on site.
- Where required ensure the fire alarm is isolated to prevent any false activations.

9. DOCUMENTATION

9.1. General

The Contractor is to be aware there are no O&M drawings for the currently installed ACS.

The Contractor shall submit a draft copy of their own Operations and Maintenance (O&M) manual to the Employer for approval. The draft copy is to be delivered two (2) weeks before handover of the system. The draft copy shall be delivered in electronic format. All comments made by the Employer shall be included into the document and the draft resubmitted. When the draft documentation has been approved, formal copies shall be issued.

The Contractor is to deliver the formal copy of the manuals within fourteen (14) days after completion of the witness testing of all systems. The final copy of the Operations and Maintenance (O&M) manual shall be delivered in electronic format along with one (1) printed set that is to be held with HMG on site.

9.2. Crib Sheet

The Contractor is to provide a crib sheet on the basic functions of the ACS to support staff in the use of the system. The Crib sheet is to be provided for the first training session conducted

The Cribb sheet is contain as a minimum the following: -

- Adding a Cardholder
- Editing a Cardholder
- Removing a Cardholder
- Blocking a Cardholder
- Active Directory Integration Procedures
- Opening a Door
- Unlocking a Door
- Basic Report Viewing

9.3. Operations and Maintenance (O&M) Manual

The Operations and Maintenance (O&M) manual shall contain the following: -

9.3.1. Product Information & Manuals

The Contractor shall provide product data that includes, but not limited to, the following: -

- Manufacturer's technical data for all equipment installed
- Manufacturer's installation manual
- User Guides (Operator and Manager) for all hardware and software installed

For the following systems: -

- Access Control System (Software and Hardware)
- Key cabinet (If installed)

9.3.2. Asset Register

The Contractor shall provide an asset register that includes, but not limited to, the following: -

- Description of equipment
- Make and model
- Serial number
- Version of software / firmware (where applicable)
- Location of equipment
- IP Addressing

9.3.3. Schedules

The Contractor shall provide an updated schedule for the following: -

- All connected ACS Doors

9.3.4. Drawings

The Contractor shall provide 'as-built' drawings in AutoCAD (.dwg) format for the ACS.

9.3.5. Maintenance

The Contractor shall provide a maintenance schedule section that includes descriptions of maintenance for all equipment including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

9.3.6. Usernames & Passwords

The Contractor shall provide a maintenance section that includes the username and password of all equipment that requires a logon. These must include any Administrator / Supervisor or engineering username and password details.

10. COMPLETION & HANDOVER

10.1. Training

The Contractor is to provide comprehensive training for HMG staff on the new ACS.

The training is to be conducted in person at the Museum and not via an online meeting.

The Contractor is to issue a training program itinerary two (2) weeks prior to the delivery of the training to be approved by the Employer.

It is expected there will be two different training sessions.

The first training session is to be conducted when the ACS software has been installed and linked to the HMG Active Directory so staff cardholders have already been populated into the new ACS.

This first training session is to ensure that all of the required cardholders have been entered into the ACS system, credentials issued, ahead of the exchange of the door controllers and credential readers.

It is then expected the second training session will be for twelve (12) staff that require a one (1) day operator training.

This second training session is to ensure that all of the required staff know how to operate the ACS for day to day operations.

The operator training is to be split into three (3) sessions with four (4) staff in each session.

The Contractor is to provide a hard copy of the operator manuals and a training guide for all equipment.

The training is completed prior to the new ACS becoming operational so the transition to the new systems will be as seamless as possible.

The training provided shall be delivered by a competent person who is capable of delivering a training program that covers all of the ACS functions required by HMG staff.

Once completed the Contractor shall issue documentation to the Employer confirming what training has been delivered and to whom in HMG

10.2. Commissioning

The Contractor shall fully commission the following connected systems: -

- Access Control System
    - All Connected Door Controllers
    - Peripherals
    - ACS Server Software
    - Client Workstations

10.3. Witness Testing

The Contractor shall invite the Client and/or Client's Representative to carry out an inspection of the installation at times when project tasks have been completed.

The Contractor shall provide two (2) weeks before the witness testing date documentation for the witness testing. The documentation is to include all of the connected doors during the witness testing a random number will be selected and tested to ensure the system is functioning as required.

The Client and/or Client's Representative will witness test the following: -

- All connected Access Control Door operate as expected

If any defects are recorded by the Client and/or Client's Representative these shall be corrected by the Contractor.

Once all defects are resolved by the Contractor, the Contractor shall notify the Client that all works are complete in compliance with the specification.

10.4. Final Acceptance and Handover

Final acceptance and handover of the ACS shall not be given until the following have been carried out to the satisfaction of the Employer: -

- Rectification of snagging report
- Completion of training programme

10.5. Completion

The Employer shall award Completion of the project following completion of the acceptance and handover of HMG.

A signed Completion certificate shall be issued to the Contractor stating the date of Completion and the start/end of the defects period.

The Employer shall decide when Completion shall be granted.

10.6. Defects Warranty

The Contractor shall provide within their proposal sum a twelve (12) month defects liability and system warranty for every component of the new ACS

This warranty shall include for the Contractor to attend site to repair or replace fault components of the ACS and to return the system to full working order.

11. SERVICE AND MAINTENANCE

The Contractor is to provide costs for an optional one (1) year Maintenance and Software support Agreement. The Maintenance contract is to run concurrently with the Defects Liability Period (DLP) of the new equipment, which will expire 12-months after the Acceptance of the new System.

The Contractors Maintenance Agreement is to include the following: -

- Two (2) Planned Preventative Maintenance (PPM) visits per year to check the operations of every ACS door. These checks are to include ensuring all locking mechanisms are secure.
- All software and firmware updates to all ACS server, workstations and all ACS equipment is carried out

The Contractor is to provide costs for the following level of Reactive Maintenance Agreement: -

- Monday-Friday 0800-1700 (excluding weekends and public holidays) maintenance contract including labour, plant and tools

The Contractor is to include their Maintenance Agreement as part of the proposal which include the responses times expected for a callout

END OF SPECIFICATION