Technical Specification

Access Control and Building Monitoring System
To be installed at

_____

TABLE OF CONTENTS

1 General Requirements

1.1 Operating system platform

It is an express requirement of this tender that the contractor shall offer an integrated Access Control and building Monitoring System (ACBMS) which is optimised to operate in a Microsoft Windows XP Professional operating system environment. The ACBMS software application shall be designed to utilise the latest features provided by the Windows graphical user interface (GUI). Software applications for DOS or 16-bit versions of Windows, shall not be acceptable.

1.2 Computer hardware platform

The computer hardware offered for servers and workstations shall comply with recommendations as laid down by the manufacturer of the ACBMS. In addition, it is specifically required that the computer hardware shall employ a central processing unit (CPU) manufactured by Intel Corporation. Computer hardware employing CPUs from other manufacturers shall not be acceptable. Furthermore, the contractor shall provide guarantees that all computer equipment (including expansion boards and peripherals) is compatible with the Windows XP Professional operating systems.

1.3 Compatibility of access control hardware and Software

Tenderers are advised that preference will be given to systems employing access control hardware and software provided by a single vendor. In an event, it shall be incumbent upon the tenderer to prove that the proposed combination of hardware and software has been implemented successfully in other installations of similar size and functionality to the system specified herein.

1.4 System integration and extensibility

The ACBMS shall employ the latest available open database technologies to provide a transparent interface to the system database. These database technologies shall allow the ACBMS to interface with any database management system that provides an interface which complies with the OLE DB specification. It is a specific requirement that access control event logs and system event logs shall be able to be stored using common database management system, including Microsoft Access, Microsoft SQL Server, Informix and Oracle.

The architecture of the ACBMS shall allow the modular implementation, commissioning and decommissioning of segments of the system to suit client requirements. It shall be possible to install the ACBMS on several controllers located arbitrarily across the site. Each controller shall be capable of operating independently of other controller's. However, the

system shall allow the integration of all controllers. The system shall be capable of consolidating tagholder and card reader transaction data from separate controllers into a central data store. It is a specific requirement that anti-passback functionality (as described elsewhere in this specification) be maintained at all times across all controllers on which the ACBMS is installed.

1.5 Vendor and installer credentials

The software vendor shall preferably be accredited by the ACBMS manufacturer. The tenderer shall be certified by the access control hardware and software vendor as an approved installer of the proposed ACBMS. In addition, the tenderer shall, for a period of at least two (2) years after completion of the contract, employ at least two (2) technicians who have completed appropriate factory training and are properly certified to support the proposed ACBMS. It shall be incumbent upon the tenderer to prove compliance with these requirements.

.

2 Access Control Software

2.1 Graphical user interface

The ACBMS application software shall provide a graphical user interface to the functionality provided by all access control hardware that forms part of the proposed system. The system shall also provide the capability to interface with and control other security subsystems (including, but not limited to CCTV surveillance systems).

At a minimum, the ACBMS shall provide graphical tools for:

- System administration and maintenance
- Configuration of access control hardware
- Administration of tag/card holders
- Management of access control for access groups
- Assigning operator permissions

2.2 Application settings

Administrators shall be able to configure the ACBMS software by invoking a software configuration ("option") module. The software configuration module shall provide a graphical interface enabling administrators to configure various aspects of the application, including:

- Location of database files
- Logging of access control events, system events, and time and attendance data
- Behaviour of key software modules
- Definition of tag holder access levels using access groups(to facilitate greater control of high security areas)
- Access control groups for tag holders
- Labels of user-defined data fields

2.3 User administration

The ACBMS shall employ user groups to control the permissions of individual users and groups of users. Administrators shall be able to control access to the system's functionality by creating user groups, defining the permissions of those user groups and adding members to those groups. It shall be possible to specify the date from which a member of a group will be a valid user and the period for which he or she will remain a valid user.

The software shall allow administrators to control which tag holders, access control groups, readers and zones a specific user group is authorised to manage. Systems that employ access level mechanisms or

require administrators to configure permissions separately for each user, shall not be acceptable.

The ACBMS shall maintain a detailed record of each user login, including information about all actions performed by the user. The system shall store application and interface configuration settings for each user, and present the user interface according to the settings specified for each user.

2.4 Language support

The proposed ACBMS software application user interface shall be available in English.

2.5 Tag holder management

The ACBMS shall provide fully integrated functionality for the recording of tag holder information and the issuing of cards

2.5.1 Group control

It shall be possible to manage access control and monitor activity of individual tag holders and groups of tag holders. Group management functionality shall include the facility to administer an entire group of tag holders as a single entry. Authorised users shall be able to specify the zones and readers where a tag holder group will be allowed access, as well as one or more schedules specifying the period(s) for which the group will have access to each zone or reader.

It shall be possible to enable or disable a group. When a group is disabled, the access control permissions of the entire group shall be suspended. Administrators shall be able to specify any group as a "T&A group", thus enabling logging of basic time and attendance data for that group. In addition, the ACBMS application software shall enable administrators to override zone control and/or anti-passback for any group.

2.5.2 Support for companies/departments

It shall be possible to define any number of separate companies within the ACBMS. The software shall also provide an option enabling administrators to define departments within each company. The tag holder management modules shall enable operators to specify the company and department to which a tag holder belongs. It shall be possible to associate one or more tag holders with a company/department by selecting the tag holders in the relevant in the relevant tag holder management module and adding the selection to the company/department management module. Each company shall have an expiry date whereby all members of the company's access permissions will expire.

2.5.3 Tag holders

Tag holder management module shall provide an interface allowing users to manage all data pertaining to tag holders.

2.5.3.1 Tag holder control

Administrators shall be able to assign control of any tag holder group to any user group. A user's ability to control tag holder records and access control permissions shall be controlled by permissions set for the user group(s) of which that user is a member. Duly authorised operators shall be able to assign zone and reader access permissions simultaneously to the members of an entire access group.

2.5.3.2 Tag holder data

Data accessible from the tag holder management module shall include the following types of information:

- Personal details (e.g. title, first names, surname, employee number, ID number, gender)
- ID cards and/or Personal Identification Numbers (PINs) assigned to the employee
- Unique ID card number of up to 32 digits
- Card validity, time and attendance logging options
- Photographs
- Contact details
- Company and department to which employee is assigned
- Access groups to which tag holders belong. The access group/s shall assign permission to zones and readers as well as schedules specifying the periods during which a tag holder will be granted access at a specific zone or reader

In addition to these standard data fields, the tag holder record shall provide any amount of additional fields for the entry of user-definable data. These additional fields shall be definable to be a combo box, automatically populated dropdown lists, text fields, memo fields or additional photograph fields.

2.5.3.3 Card assignment

Operators shall be able to assign an ID card from within the employee management module by activating a take-on reader connected to the workstation. Any access control reader shall be able to be specified as a take-on reader while still performing its access control function. It shall be possible to assign multiple ID cards to an employee and to assign an alias name to each additional card.

A duly authorised operator shall be able to issue a temporary card to a tag holder. When a temporary card is issued, it shall inherit the access control permissions that have been defined for the tag holder primary card. The operator shall also be able to specify that any card be deposited in a drop box when the cardholder exists at a specific reader. The system shall automatically consolidate time and attendance data for all cards (including temporary cards) issued to a tag holder.

It shall be possible to specify the activation and expiration times of a card unambiguously in hours, minutes and seconds on any day of the month of any year in the future (e.g. 2000/12/31, 23:59:59). Operators shall also be able to specify that a card expires at the end of the day on which it is issued.

2.5.4 Image capture

It shall be possible to capture or import digitised video images and associate them with tag holder records. The system shall provide support for the capturing of images at any resolution that is supported by the hardware used to capture the images. At a minimum, the software shall provide functionality enabling operators to crop and resize captured or imported images. Image enhancement functionality is not required.

2.5.5 Card printing

Card printing functionality shall be accessible directly from the ACBMS application software. Systems that require specialised manipulation or export of data for the issuing of cards shall not be acceptable.

2.5.6 Tag holder take-on stations

The software vendor shall provide a tag holder take-on module that enables users with limited computing experience to view, edit and add records to the tag holder database and to assign cards to tag holders. The personnel take-on module shall provide functionality that allows operators to:

- Enter detailed information about tag holders using a set of administrator-configurable data entry screens
- Preview input from a video camera connected to the take-on station, capture a frame, and link it to a tag holder data record
- Ascertain the location of any visitor or employee by displaying a list of all tag holders who have passed through access points
- Capture images using a TWAIN compatible device.

- Restrict a tag holder to specified areas by assigning an access control group defining permissions for that tag holder
- Specify the period for which a tag holder's card is valid
- Print personalised tag holder cards to a suitable printer connected to any workstation on the local area network
- Control precisely the placement of multiple cards on a page

The personnel take-on station shall include a card design facility whereby cards can be fully and completely designed. This design facility shall have the capability to import picture files. Systems where additional modules or software applications is required to design cards shall be unacceptable.

The functionality available on personnel take-on stations shall depend on permissions and configuration data assigned to a user group by the system administrator. Operators shall be required to log on to personnel take-on stations by entering user names and passwords.

2.6 Site configuration

The ACBMS shall provide administrators with the capability to configure a system using an easy to use interface that follows a logical configuration order.

2.7 System monitoring

The ACBMS software application shall incorporate modules that allow administrators and operators to monitor the status and performance of the system in real time. Specifically, modules shall be provided for the real-time viewing of access control events, the current location of tag holders.

The access control event viewer shall be able to filter real-time events for specified tag holders and/or readers, zones, access groups, etc. Users shall be able to select in which order events are displayed.

The system event viewer shall list the real-time system events that are being logged in the ACBMS database. Users shall be able to select which properties of an event are displayed and in which order they are displayed.

A personnel locations viewer shall be provided to enable operators to ascertain the current location of any tag holder. This viewer shall provide information about the last reader at which a tag holder presented their card, or at the last zone that the tag holder entered. The viewer shall have the capability to be filtered by tag holder, zone or reader, thus enabling users to monitor specific areas or specific tag holders.

2.8 Zone control

The ACBMS shall provide complete support for both reader-based and zone-based access control models. The software shall enable administrators to define a zone by selecting doors that lead to or from the zone. Administrators shall be able to assign enabling schedules to a zone to specify the time period(s) during which access shall be allowed to the zone. The system shall also be capable of enforcing strict anti-passback control by denying access to a zone if a tag holder previously entered that zone without subsequently exiting. It shall be possible for administrators and authorised operators to override the enforcement of anti-passback control for any group of tag holders. The system shall also employ a timed anti-passback feature for all or specified zones.

2.9 Counters

The ACBMS application software shall provide functionality to define counters and link those counters to any object or event defined in the system. It shall be possible to define an initial value for each counter. It shall be possible to define actions that are performed by the system when the counter is less than, equal to or greater than a specified value. Users shall have the capability to employ the object and event configuration module (as described elsewhere in this specification) to clear a counter, reset a counter, set a counter arbitrary integer value, increment or decrement a counter by 1, or increment or decrement a counter by an arbitrary integer value in response to any event generated in the system.

2.10 Time Control

The ACBMS shall allow users to configure timers and schedules that control the execution of actions, as well as schedules that specify the validity of access control permissions.

2.10.1 Timers

It shall be possible to define timers to control the behaviour of system objects. Users shall be able to specify the duration of a timer in milliseconds; start; stop or reset a timer in response to any event generated in the system; specify actions to be performed when a timer expires; and configure a timer to restart automatically after expiring.

2.10.2 Schedules

Schedules shall provide the capability to generate events that control the behaviour of objects defined in the system. Each schedule shall comprise one or more time entities, each of which shall activate events in one of the following ways:

- At a specific time on a specific day
- Weekly at a specific time on a specific day of the week
- Daily at a specific time on one or more days of the week
- Hourly at a specific number of minutes after the hour

The ACBMS software shall enable users to specify the period for which any set of access control permissions is valid by associating a schedule or combination of schedules to those access control permissions. As mentioned elsewhere in this specification, it shall be possible to use schedules to specify the validity of zone permissions or reader permissions for any group of tag holders.

It shall be possible to define access control schedules that span periods of seven days (from 00h00 on Monday to 23h59 on Sunday) and comprise any combination of valid time entities (i.e. start and end times) within the relevant seven-day period. It shall also be possible to define schedules that start and end at any time on any day. In addition, users shall have the capability to define complex schedules comprising several period schedules which recur in a user-definable sequence.

2.11 Time and attendance functionality

The ACBMS software application shall incorporate support for the acquisition, recording and exporting of basic time and attendance data for all tag holders.

Administrators shall have the option to enable or disable the acquisition of time and attendance data at any reader defined in the system. The software shall also allow users to enable or disable the recording of time and attendance data for any tag holder group.

The ACBMS software shall be capable of exporting time and attendance data in a range of standard formats supported by commonly used time and attendance software applications.

2.12 Offline functionality

The ACBMS shall be a fully off-line system. All access control functions shall be done at door controller level. Systems requiring access control functionality to be controlled by a computer shall be unacceptable.

In addition to this, all system objects i.e. counters, timers, inputs, outputs and schedules shall be stored at the door controllers. The ACBMS software shall merely be an interface to provide an easy to use management and configuration tool for the end-user as well as provide data storage. All functions that include the modifying of tag holder access permissions and additional non-administrative functions shall be downloaded to the door controllers seamlessly and intelligently. The system shall not download all information to all controllers whether on demand or automatically. Only

the relevant information required for a specific door controller shall be downloaded to that specific door controller.

The user shall not be required to manually start an upload process to retrieve transaction logs. This operation shall be performed automatically by the system in the event that the connection to the door controller was lost and has been restored. Should a connection be lost, the door controller shall have full functionality regarding access control or event management. The system will inform the user when a connection to a door controller is lost.

2.13 Data administration and backup

Users shall have the ability to import tag holder data from a variety of delimited flat ASCII files. The system shall automatically identify duplicate data entries, alert the user to the existence of such duplicate entries, and prompt the user to select which entries should be retained and which entries should be discarded.

The ACBMS shall provide tools that enable users to verify and maintain the integrity of the system database.

Backup and restore facilities are not provided as part of the ACBMS. It shall be incumbent upon the system installer to design and implement appropriate backup procedures.

2.14 Report generation

It shall be possible for authorised users to extract reports from the ACBMS.

3 Access Control Hardware

3.1 PC/door controller interface

The access control hardware vendor shall supply a system that does not require PC adapter cards to provide interface between the proposed door controllers and the PC on which the ACBMS software application is installed. Systems that employ PC adapter cards for communication between door controllers and the PC shall be unacceptable. Door controllers shall be capable of connecting to the PC via a RS232 serial interface or a TCP/IP Ethernet connection.

The architecture of the networking system shall allow controllers to be connected in a multi-dropped topology using standard Mylar, UTP CAT 4 or CAT 5 copper cabling. The hardware vendor shall also provide equipment that allows for the implementation of the proposed networking system on fibre optic cabling where connectivity is required over distances longer than those typically supported by copper cabling.

It is a requirement of this tender that the system PC/door controller interface has the capability to support reliable data acquisition from card readers and door controllers while the system is operating at a load of 5000 card reader transactions per hour.

3.2 Door controllers

A network of door controllers shall be employed to provide a complete interface to functionality available on those door controllers. The use of networked door controllers shall also facilitate the modular implementation of portions of the ACBMS as required by the client.

Door controllers shall provide full offline functionality. (Online mode is defined as a mode in which access control decisions are made by the central ACBMS server computer. Offline mode is defined as a mode in which access control decisions are made by the door controller based on locally stored system configuration and card permissions data). The door controller shall be capable of functioning fully in the offline mode. Even if there is no connection to the PC, the door controllers shall continue to process requests for access received from card readers to the door controller.

Each door controller shall have the capacity for the storage of 3200 tag holders without using any expansion modules. Memory expansion modules connected to the door controllers via expansion headers shall increase the tag holder capacity to at least 25000 tag holders. The stored tag holders shall be configurable tag holders whose access permissions can be modified or completely removed. Systems that employ a range of tag numbers for access to certain sites shall be unacceptable.

Door controllers shall store all event transactions. Once a connection is established all transaction logs will automatically be uploaded to the database on the computer. All door controllers shall be capable of TCP/IP

connectivity and RS232 Serial connectivity and will use this as a method of communication to the computer.

Door controllers shall be housed in lockable metal enclosures that can be mounted on a variety of flat surfaces. Door controllers shall be capable of operating at ambient temperatures ranging from 0°C to 50°C.

The tenderer shall recommend door controllers based on a thorough assessment of the requirements of the installation.

The hardware vendor shall provide controllers with the following configurations of inputs and outputs:

- Digital inputs and changeover relay outputs

3.2.1 AC-powered door controllers with digital inputs and relay outputs

The tenderer shall install door controllers that can store at a minimum 3200 tag holders without expansion modules and that is equipped with 6 digital inputs, 1 fire input, 1 tamper input and 5 digital outputs of the changeover relay contact type. A digital input shall be switched on when a voltage in the range 0VDC – 12VDC is present across the input. Each relay output shall be rated for a maximum switching voltage of 220VAC and a maximum (non-inductive) switching current of 2A. The status of each input and output point shall be indicated in real time by an individual LED. LEDs shall also be provided to indicate CPU activity, network status and power conditions. In addition, the system controller shall be equipped with a real-time clock. These door controllers shall be capable of operating on a 220VAC 50Hz mains power supply.

3.3 Read/write proximity smart card infrastructure

3.3.1 RS485 proximity smart card read/write terminals

Read/write terminals shall be capable of communicating at a frequency of 125kHz with proximity cards that are presented within approximately 100mm of the front of the unit.

Each proximity read/write terminal shall incorporate an LED capable of displaying blue, green, red and amber in response to outputs generated by the ACBMS via the card reader controller. Proximity read/write terminals shall also be equipped with internal piezzo-electric buzzers capable of generating audible tones to indicate the response of the ACBMS to the presentation of an identification card.

Read/write terminals shall be connected to door controllers by means of a standard RS485 serial interface supporting bi-directional data communications at a rate of 9600 bits per second. The bi-directional RS485 interface shall allow the full implementation of the latest available non-contact read/write smart card technology.

Read/write terminals shall provide a convenient mechanism (such as a rotary DIP switch) for the selection of the terminal's unique address on the serial network.

Read/write terminals are required to provide support for the Phillips HITAG™ 1 & 2 and EM Marin H4002 proximity protocols. Read/write terminals shall also be equipped with field-changeable firmware, allowing the terminals to be reprogrammed in order to accommodate changes in proximity transponder technologies.

Read/write terminals shall be capable of functioning when mounted directly on metal surfaces.

Read/write terminals shall be able to communicate via RS485 and as a Wiegand device.

