# TABLE OF CONTENTS

1. **GENERAL** ........................................................................................................................................................................... 10
   
   1.1 General Installation Requirements ................................................................................................................................. 10
   
   1.1.1 General ........................................................................................................................................................................... 10
   
   1.1.1.7 Cable Damage ........................................................................................................................................................... 11
   
   1.1.1.3 Cable Numbering ...................................................................................................................................................... 11
   
   1.1.1.4 Co-ordination and Separation of Services .................................................................................................................... 11
   
   1.1.1.5 Co-ordination and Feasibility ...................................................................................................................................... 11
   
   1.1.1.6 Special Cabling ........................................................................................................................................................... 12
   
   1.1.1.7 Wiring Diagrams ...................................................................................................................................................... 12
   
   1.1.1.8 Coaxial Cabling ........................................................................................................................................................ 12
   
   1.1.1.9 Fibre Optic Cabling ................................................................................................................................................ 12
   
   1.1.1.9.1 Other Security Services Fibre Optic Requirements ................................................................................................ 13
   
   1.1.1.9.2 Fibre Optic General .............................................................................................................................................. 13
   
   1.1.1.9.4 Fibre Optic Splice Box (FOSB) .................................................................................................................................. 15
   
   1.1.1.9.5 Fibre Optic Cable and Equipment Testing ............................................................................................................... 16
   
   1.1.1.9.6 Spider Diagrams ...................................................................................................................................................... 17
   
   1.1.2 Earthing Specification .................................................................................................................................................. 18
   
   1.1.3 Lighting and Surge Protection Specification .................................................................................................................. 19
   
   1.1.3.1 General ...................................................................................................................................................................... 19
   
   1.1.3.2 TVSS Technology – AC Power Applications ............................................................................................................. 19
   
   1.1.3.3 TVSS Technology – DC Power Applications ............................................................................................................. 19
   
   1.1.3.4 Application ............................................................................................................................................................... 19
   
   1.1.4 Equipment Fixing Requirements .................................................................................................................................. 20
   
   1.1.4.1 Specific Surface Requirements .................................................................................................................................. 20
   
   1.1.4.1.1 Drywall ................................................................................................................................................................. 20
   
   1.1.4.1.2 Brick walls ............................................................................................................................................................ 20
   
   1.1.4.1.3 Concrete ............................................................................................................................................................... 20
   
   1.1.4.1.4 Ceilings .................................................................................................................................................................. 20
   
   1.1.4.1.5 Steel ....................................................................................................................................................................... 21
   
   1.1.4.1.6 Wood ..................................................................................................................................................................... 21
   
   1.1.4.1.7 Aluminium ............................................................................................................................................................ 21
   
   1.1.4.2 Specific equipment instructions ..................................................................................................................................... 21
   
   1.1.4.2.1 Alarm wire ........................................................................................................................................................... 21
   
   1.1.4.2.2 Trunking ............................................................................................................................................................... 21
   
   1.1.4.2.3 Conduits .............................................................................................................................................................. 21
   
   1.1.4.3 Tamperproof Screws, Bolts and Nuts ........................................................................................................................... 21
   
   1.1.5 Signs, Markers, Nameplates and Tags ........................................................................................................................... 23
   
   1.1.5.1 Cable Tags ................................................................................................................................................................. 23
   
   1.1.5.1.1 General ................................................................................................................................................................. 23
   
   1.1.5.1.2 Cable Tagging Requirements ................................................................................................................................ 23
   
   1.1.5.2 Nameplates ............................................................................................................................................................... 24
   
   1.1.5.3 Zone Identification Markers ...................................................................................................................................... 24
   
   1.1.5.4 Electrified Fence Warning Signs .................................................................................................................................. 25
   
   1.1.6 19" Racks ....................................................................................................................................................................... 25
   
   1.1.6.1 General ...................................................................................................................................................................... 25
   
   1.1.6.2 Installation Requirements and Layout ....................................................................................................................... 25
   
   1.1.7 Wall Mount 19" Racks .................................................................................................................................................... 27
   
   1.1.8 19" Rack Accessories ...................................................................................................................................................... 28
   
   1.1.8.1 Brush Panels ............................................................................................................................................................. 28
   
   1.1.8.2 Cable Routing Panels .................................................................................................................................................. 28
   
   1.1.8.3 Cable Routing Rings ................................................................................................................................................... 29
   
   1.1.8.4 Cable Jumpering Bracket ............................................................................................................................................ 29
   
   1.1.8.5 Shelf ............................................................................................................................................................................ 30
   
   1.1.8.6 Pull-Out Shelf .............................................................................................................................................................. 30
   
   1.1.8.7 Blank Panels ............................................................................................................................................................. 31
   
   1.1.8.8 Brush Covers ............................................................................................................................................................ 31
   
   1.1.8.9 Mounting Materials .................................................................................................................................................... 31
   
   1.1.8.10 Power Strips (Multi-plugs) ....................................................................................................................................... 32
   
   1.1.8.10.1 19" Horizontal Mounting Option ......................................................................................................................... 32
   
   1.1.8.10.2 19" Vertical Mounting Option .................................................................................................................................. 33
   
   1.2 Computer Hardware ............................................................................................................................................................ 33
   
   1.2.1 Operator Workstations, Card Printing Stations and Servers ............................................................................................ 33
   
   1.2.1.1 Torture / Stress Testing Hardware ................................................................................................................................... 33
   
   1.2.1.2 Operator Workstations ................................................................................................................................................ 33
   
   1.2.1.3 Card Printing / Take-On Stations ................................................................................................................................... 34
   
   1.2.2 Servers ............................................................................................................................................................................. 34
   
   1.2.2.1 Medium Installation CCTV Recorder and Virtual Server .......................................................................................... 34

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©

---

**GENERAL SPECIFICATION FOR THE ACCESS CONTROL PORTION OF THE INTEGRATED SECURITY SYSTEM AT THE DTI**

31 MAY 2018

PAGE 1/1
2 PHYSICAL SECURITY INFORMATION MANAGEMENT (PSIM) SYSTEM........................................... 71

2.1 PSIM Overview ..................................................................................................................... 71
2.2 Mandatory Requirements ..................................................................................................... 71
2.3 Future Capabilities ................................................................................................................ 73
2.4 Quality Assurance ................................................................................................................ 73
2.5 Product .................................................................................................................................. 73

2.5.1 Software Components ....................................................................................................... 73
2.5.2 Device Assets ....................................................................................................................... 73
2.5.3 Alarm Management ............................................................................................................ 73
2.5.4 Triggers ................................................................................................................................ 74
2.5.5 Alarm Stack ......................................................................................................................... 75
2.5.6 Dashboard ........................................................................................................................... 75
2.5.7 Map Functionality ............................................................................................................... 75
2.5.8 Video Display ...................................................................................................................... 76
2.5.9 Video Playback .................................................................................................................... 76
2.5.10 Video Display Permissions ............................................................................................... 76
2.5.11 Video Display Sequences .................................................................................................. 77
2.5.12 Video Display Tile Layouts ............................................................................................... 77
2.5.13 Pan Tilt Zoom Control ....................................................................................................... 78
2.5.14 Video Export ...................................................................................................................... 78
2.5.15 Video Wall Display ........................................................................................................... 79
2.5.16 Contacts and Contact Groups ......................................................................................... 79
2.5.17 Data Access ...................................................................................................................... 79
2.5.18 Reporting Services ........................................................................................................... 80
2.5.19 Scalability Architecture .................................................................................................... 80
2.5.20 Virtualisation Architecture ............................................................................................... 80
2.5.21 Federation ......................................................................................................................... 81
2.5.22 Failover Architecture and High Availability ....................................................................... 81
2.5.23 Email ................................................................................................................................ 81
2.5.24 SNMP ................................................................................................................................ 81
2.5.25 Workflow .......................................................................................................................... 81
2.5.26 Sub-System Integration ...................................................................................................... 83
2.5.27 Integration SDK ................................................................................................................ 84
2.5.28 Audit Trails ....................................................................................................................... 84
2.5.29 Users and Permissions ...................................................................................................... 85
2.5.30 Graphical User Interfaces ................................................................................................. 87
2.5.31 Localisation ..................................................................................................................... 89
2.5.32 Administration Interface ................................................................................................... 89
2.5.33 Configuration Interface .................................................................................................... 89
2.5.34 Security Policies .............................................................................................................. 90
2.5.35 Web ................................................................................................................................ 90
2.5.36 APP for Tablets and Cell Phones ...................................................................................... 91
2.5.37 Process Guidance ............................................................................................................. 91
2.5.38 Technology Platform ....................................................................................................... 91
2.5.39 System Infrastructure ....................................................................................................... 91
2.5.40 Operating System Requirements .................................................................................... 91
2.5.41 Software Licensing Requirements ................................................................................... 92
2.5.42 Execution ......................................................................................................................... 92
2.5.43 Functional Capabilities ..................................................................................................... 92
2.5.43.1 General ......................................................................................................................... 92
2.5.43.2 Generic Web Page Viewer ............................................................................................ 93
2.5.43.3 Reporting ...................................................................................................................... 93
2.5.43.4 Escalation ...................................................................................................................... 93
2.5.43.5 Alarm Activities ........................................................................................................... 93
2.5.43.6 Alarm Events ............................................................................................................... 94
2.5.43.7 Alarm Point Suppression .............................................................................................. 94
2.5.43.8 Door Options ............................................................................................................... 94
2.5.43.9 Process Guidance ........................................................................................................ 94

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
3.2.4.5.6 Swipe Sequencing
3.2.4.5.7 Reader Monitoring
3.2.4.5.8 Random Employee/Student / Visitor Search Functionality
3.2.4.5.9 Visitor and Employee/Student Take-On Stations
3.2.4.5.10 Site Configuration
3.2.4.5.11 Object and Event Control
3.2.4.5.12 System Alarm Management
3.2.4.5.13 System Monitoring
3.2.4.5.14 Intrusion Alarm Control
3.2.4.5.15 Offline Functionality

3.2.4.6 User Interface
3.2.4.6.1 Search
3.2.4.6.1.1 Advanced Search
3.2.4.6.1.2 Search Results
3.2.4.6.2 Status Viewer
3.2.4.6.3 Alarm Viewer
3.2.4.6.4 Event Viewer
3.2.4.6.5 Browser
3.2.4.6.6 Customization Manager
3.2.4.6.7 Report Manager
3.2.4.6.7.1 Customization Reports
3.2.4.6.7.2 Access Controller Configuration
3.2.4.6.7.3 History Logs
3.2.4.6.7.4 Person Information
3.2.4.6.7.5 SMS Configuration
3.2.4.6.8 Graphics
3.2.4.6.9 Badge and Graphics Designer
3.2.4.6.10 Enrolment Manager
3.2.4.6.11 Switch Operator
3.2.4.6.12 Add-Ins

3.2.4.7 Scheduling and Timing
3.2.4.7.1 Counters
3.2.4.7.2 Task Scheduler
3.2.4.7.3 Access Control Schedules
3.2.4.7.4 Holidays

3.2.4.8 Reporting
3.2.4.8.1 Report Generation
3.2.4.8.2 Schedule Details
3.2.4.8.3 Time and Attendance Functionality

3.2.4.9 Data Handling
3.2.4.9.1 Data Administration and Backup
3.2.4.9.2 Offline Storage
3.2.4.9.3 Database Size Limitation Settings
3.2.4.9.4 Low Storage Space Warnings
3.2.4.9.5 SQL Database Manager

4 \section*{ACCESS CONTROL HARDWARE}

4.1 General
4.2 Definitions
4.3 System Description
4.3.1 RFID Technology
4.3.2 Escutcheon
4.3.3 GEO E-Cylinder
4.3.4 Locker Lock
4.3.5 Wide Profile Mortise Lock & Strike
4.3.6 Narrow Profile Mortise Lock & Strike
4.4 Semi-Online (Wireless) Components
4.4.1 PoE Gateway
4.4.2 RS-485 Gateway
4.4.3 RS-485 Nodes
4.5 Online Access Control
4.5.1 Door Controller
4.5.2 Server / Door Controller Interface
4.5.3 Door Controllers
4.5.3.1 Door Controller Network
4.5.3.2 Door Controller Functionality and Performance
4.5.3.2.1 General
4.5.3.2.2 Memory
4.5.3.2.3 Power Supply
4.5.3.2.4 Communications Interface
4.6 Access Control Management Tools
4.6.1 Card Encoder

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelc ©
5 WIRELESS INTRUDER DETECTION HARDWARE

5.1 General .......................................................................................................................... 155

5.2 Intruder Detection Management System ................................................................. 155

5.2.1 Scope .......................................................................................................................... 155

5.2.2 General Requirements ............................................................................................. 155

5.2.3 System Operation ...................................................................................................... 155

5.2.3.1 Intrusion Detection Panels .................................................................................. 155

5.2.3.2 Intrusion Detection Zones .................................................................................... 155

5.2.3.3 Intrusion Detection Areas .................................................................................... 156

5.2.3.4 Intrusion Detection Panel Users .......................................................................... 156

5.2.3.5 Intrusion Detection On-Board Relays .................................................................. 156

5.2.3.6 Intrusion Detection Off-Board Relays ................................................................. 156

5.2.3.7 Intrusion Detection Doors ................................................................................... 156

5.2.4 Alarm Monitoring Integration .................................................................................. 156

5.2.4.1 General Alarm Monitoring Integration ............................................................... 156

5.2.4.2 Alarm View ......................................................................................................... 157

5.2.4.3 Alarm Details ....................................................................................................... 157

5.2.4.4 System Hardware Status Tree ............................................................................ 157

5.2.4.5 Intrusion Detection Tracing ................................................................................ 157

5.2.4.6 Real Time Status Indicators and Information .................................................... 157

5.2.5 Command and Control Functionality ...................................................................... 159

5.2.5.1 Intrusion Panel Commands ............................................................................... 159

5.2.5.2 Zone Commands ................................................................................................. 159

5.2.5.3 Area Commands ................................................................................................. 159

5.2.5.4 On-Board Relay Commands .............................................................................. 159

5.2.5.5 Off-Board Relay Commands ............................................................................. 159

5.2.6 System Events .......................................................................................................... 160

5.2.7 Status Requirements ............................................................................................... 163

5.2.8 Panic Push Button Alarm System ........................................................................... 165

5.3.1 Activation .................................................................................................................. 165

5.3 Intruder Detection System Components ................................................................. 165

5.3.1 Control Panel ............................................................................................................ 166

5.3.2 Control Panel Expansion Modules ........................................................................... 168

5.3.2.1 8-Zone Hardwired Expansion Module ............................................................... 168

5.3.2.2 32-Zone Wireless Expansion Module ............................................................... 169

5.3.2.3 2-Port Hub and Bus Isolator .............................................................................. 171

5.3.2.4 4-Programmable Output Expansion Module ................................................... 172

5.3.3 Keypads .................................................................................................................... 173

5.3.3.1 LCD Touch Screen Keypad ............................................................................... 173

5.3.4 Direct Connect Interfaces for the Control Panel ..................................................... 174

5.3.4.1 USB Connector .................................................................................................... 174

5.3.4.2 USB Memory Key ............................................................................................... 175

5.3.4.3 Internet Module .................................................................................................... 175

5.3.4.4 Integration Module ............................................................................................... 176

5.3.5 Connected Devices ................................................................................................. 178
7 IP INTERCOM SYSTEMS......................................................................................................................................... 196
  7.1 General ............................................................................................................................................................ 196
  7.2 System Description .......................................................................................................................................... 197
  7.3 Intercom Operations ....................................................................................................................................... 198
    7.3.1 Audio Control – Intercom Icon .................................................................................................................. 198
  7.4 Intercom Stations ............................................................................................................................................ 199
    7.5 System of Operation ..................................................................................................................................... 199
      7.5.1 General ..................................................................................................................................................... 199
        7.5.1.1 Normal Calls ....................................................................................................................................... 199
        7.5.1.2 Alarm Calls ....................................................................................................................................... 199
        7.5.1.3 Tamper Calls ..................................................................................................................................... 199
        7.5.1.4 System Error Messages and Event Logging ...................................................................................... 200
        7.5.1.5 Data Integrity .................................................................................................................................... 200
        7.5.1.6 Listen-In ............................................................................................................................................. 200
        7.5.1.7 Establishing a Call ............................................................................................................................. 200
          7.5.1.7.1 Respond to Normal Calls ............................................................................................................. 201
          7.5.1.7.2 Response to Alarm Calls ............................................................................................................. 201
        7.5.1.8 Call & Event Logging ......................................................................................................................... 201
        7.5.1.9 System Maintenance .......................................................................................................................... 201
        7.5.1.10 Multiple or Simultaneous Calls ...................................................................................................... 201
        7.5.1.11 Suppression of Calls ....................................................................................................................... 201
        7.5.1.12 Future Expansion ............................................................................................................................. 202
  7.6 Intercom Stations ............................................................................................................................................ 202
    7.6.1 Intercom Units .......................................................................................................................................... 202
  7.7 Digital Audio Recording System .................................................................................................................. 202
  7.8 Intercom Operation ........................................................................................................................................ 203

8 GENERAL INSTALLATION REQUIREMENTS ................................................................................................... 204
  8.1 Making Good .................................................................................................................................................... 204
  8.2 Installation ....................................................................................................................................................... 204
  8.3 Packaging, Transport, Loading, Storage, Site Information and Conditions ................................................. 204
  8.4 Material, Equipment and Workmanship ....................................................................................................... 204
  8.5 Programme and Progress .............................................................................................................................. 205
  8.6 Co-Operation with Other Trades .................................................................................................................. 205
  8.7 Drawings ........................................................................................................................................................ 206
    8.7.1 Approval of Drawings .............................................................................................................................. 206
  8.8 Information Required ..................................................................................................................................... 207
  8.9 Tools and Equipment ...................................................................................................................................... 207
  8.10 Storage of Equipment and Materials .......................................................................................................... 207
  8.11 Location of Equipment .................................................................................................................................. 208
  8.12 Maintenance Tools ....................................................................................................................................... 208
  8.13 Availability of Spares .................................................................................................................................... 208
  8.14 Instruction of Operator .................................................................................................................................. 208
  8.15 Operating and Maintenance Manuals ....................................................................................................... 208

9 APPENDIX A – TECHNICAL SUPPORT DOCUMENTATION ........................................................................... 210
  9.1 Workstation Icons ......................................................................................................................................... 210

10 APPENDIX C – SOFTWARE SYSTEMS ........................................................................................................... 212
  10.1 Schedule of Software Offered .................................................................................................................... 212

11 APPENDIX D – SCHEDULE OF EQUIPMENT OFFERED ............................................................................... 213

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelc ©
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BG</td>
<td>Break Glass</td>
</tr>
<tr>
<td>DB</td>
<td>Distribution Board</td>
</tr>
<tr>
<td>CB</td>
<td>Circuit Breaker</td>
</tr>
<tr>
<td>CO, C/O</td>
<td>Change Over Contact</td>
</tr>
<tr>
<td>CRT</td>
<td>Cathode Ray Tube Screen</td>
</tr>
<tr>
<td>DPS</td>
<td>Door Position Switch</td>
</tr>
<tr>
<td>GND</td>
<td>Earth Connection</td>
</tr>
<tr>
<td>HD</td>
<td>Heat Detector</td>
</tr>
<tr>
<td>KO</td>
<td>Key Override</td>
</tr>
<tr>
<td>LAN</td>
<td>10/100 Base-T Ethernet Local Area Network</td>
</tr>
<tr>
<td>MCB</td>
<td>Miniature Circuit Breaker</td>
</tr>
<tr>
<td>M</td>
<td>Magnetic Door Lock / Maglock</td>
</tr>
<tr>
<td>MS</td>
<td>Main Switch</td>
</tr>
<tr>
<td>NC, N/C</td>
<td>Normally Closed Contact</td>
</tr>
<tr>
<td>NO, N/O</td>
<td>Normally Open Contact</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>P, PROX</td>
<td>Proximity Card Reader</td>
</tr>
<tr>
<td>PCB</td>
<td>Printed Circuit Board</td>
</tr>
<tr>
<td>PSU</td>
<td>Power Supply Unit</td>
</tr>
<tr>
<td>RS232</td>
<td>Half Duplex Serial Communications Protocol</td>
</tr>
<tr>
<td>RS-485</td>
<td>Full Duplex Serial Communications Protocol</td>
</tr>
<tr>
<td>SD</td>
<td>Smoke Detector</td>
</tr>
<tr>
<td>TTL</td>
<td>Transistor Transistor Logic</td>
</tr>
</tbody>
</table>
1. **GENERAL**

Installation Requirements and Rules

1.1 **GENERAL INSTALLATION REQUIREMENTS**

NO DEVIATION FROM THE SPECIFICATION will be tolerated or paid for without the written approval of the Engineer.

The installation shall comply in each instance with the requirements as set by the CLIENT, in particular to the general access specifications for the access control, C.C.T.V systems, intruder detection system, smoke detection and Public address and evacuation specifications, as well as all relevant SABS codes of practice and standards.

Where no SABS guideline exists the IEC and ANSI standards will be applicable.

The installation shall be done in accordance with the drawings issued by the Engineer as approved by the Client and no installation work shall be carried out without issued for construction drawings.

All routing requirements and conduit installation work shall be done by the Electrical Contractor and all additional reticulation routes required by the tenderer shall be indicated and marked on his tender submission during the time of tender.

At the end of each day, the Contractor shall be responsible for the clean up, removal, and secure disposal of all debris.

1.1.1 **CABLING**

1.1.1.1 **GENERAL**

Supply, install, connect, and terminate all cabling necessary to complete the installation, including all power and UPS distribution, audio, data, control, fibre-optic (where applicable), communications cabling and device cabling.

All cabling shall be supplied and installed as a part of this Sub-contract.

All terminated cabling shall be neatly tied/loomed to prevent damage to terminations and interference or obstruction of other services.

Strain relief shall be provided for cables connected to rack mounted equipment.

All cables shall have stranded copper conductors and shall be PVC insulated with overall PVC sheath, unless otherwise specified.

All cabling shall be concealed and installed on metal cable tray, cable duct and conduits.

Cabling shall be installed with due regard to future removal and replacement of cables.

All cables shall be new and delivered on site in unbroken reels, and with the "manufacturer's" label attached.

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

Installation and cable route shall be to the satisfaction of the Engineer.

Cables shall be installed in a manner eliminating any possibility of strain on the cable itself or on cable terminations.

No joints or connections will be permitted. Adequate loose cable shall be left behind all equipment to facilitate removal for inspection, adjustment or replacement.
Coaxial cable for CCTV cameras shall be 75 Ohm impedance with pure copper centre conductor and pure copper braided shield providing minimum 95% braid coverage.

1.1.1.2 CABLE DAMAGE

During the installation of cable should any kinks or abrasions to insulation, braiding, sheathing or armoring occur, the affected cable shall be withdrawn and replaced with new cable.

1.1.1.3 CABLE NUMBERING

Generally all cables shall be allocated and identified with unique cable number. All cables including patch leads shall be clearly labeled. Labels shall be affixed within 250 mm of each termination.

Cables shall be fitted with tags at the following points:

(a) On the cable sheath next to the gland at each end.
(b) In cable pits.
(c) At any additional point on the cable sheath (or around the core bunch) where the preceding requirements are not readily traceable from the core terminations.

Cable identification tags shall be orientated uniformly to read left to right from the logical viewing point horizontally; and from bottom to top viewed from the right where installed vertically.

Duplication of cabling and equipment identities shall not be allowed.

1.1.1.4 CO-ORDINATION AND SEPARATION OF SERVICES

Install services for each respective section and system and physically separate from other systems to a discipline and coordinated layout plan. Adjacent services shall run approximately parallel. Crossing services shall cross at approximate right angles.

Individual services between common points of the work shall follow similar parallel routes. Cables shall be parallel to the building major axes.

Separation distances shall not be less than the following:

(a) Power cables - 100mm.
(b) ELV and Communication cables to parallel power cables - 300mm.
(c) ELV and Communication cables to power cables crossed at 900 - 100mm.
(d) Any trade to finish floor level - 80mm.
(e) Any trade to structure - 20mm.

1.1.1.5 CO-ORDINATION AND FEASIBILITY

The drawings, schematics and specification indicate the main routes and positions for the various services installations and equipment in relation to the building and other services.

Check the details shown on the drawings and co-ordinate the detail layout with the building structure and other services. Submit full details of proposed major cable routes for approval before proceeding.

1.1.1.6 SPECIAL CABELING
Where equipment to be supplied and installed under this specification requires special cabling (i.e. screened cables, unshielded twisted pair, coaxial, optical fibre or other special types of cable), these cables shall be provided as part of this Sub-contract.

It shall remain the responsibility of the Sub-contractor to design the cabling system network and determine the type of cable required for interconnection of the various components, which make up the total system to be installed, to comply with the Sub-contract documents.

1.1.1.7 WIRING DIAGRAMS

Deliver to the Head Contractor in accordance with the scheduled works program:

(a) Details of all types of cabling to be installed as part of the Sub-contract works.
(b) Block schematic cable diagrams indicating all system interconnecting cables including cable routes and cable types complete with core make up and numbers.
(c) Detailed floor plans indicating cable routes and designated circuit identification.
(d) Wiring diagram detailing system interconnections and cable/core identification.

1.1.1.8 COAXIAL CABLEING

Coaxial cabling used for the purpose of Closed Circuit Television (CCTV) within buildings or other approved short haul distances shall, as a minimum be RG-59U with a solid copper core and 95% copper braid shield. The copper shall have less than 2.0% impurities. All BNC type connectors used on this cable shall be crimp type connectors.

1.1.1.9 FIBRE OPTIC CABLEING

Fiber Connector Styles

<table>
<thead>
<tr>
<th>Connector Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST Connector</td>
<td>A shielded bayonet type connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>SC Connector</td>
<td>A push/pull type connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>FC Connector</td>
<td>A shielded connector type connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>SMA Connector</td>
<td>A connector type connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>FDDI Connector</td>
<td>A push/pull type connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>Mini-BNC Connector</td>
<td>A mini-BNC connector using the traditional BNC connection method.</td>
</tr>
<tr>
<td>Biconic Connector</td>
<td>A biconic connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>MT-RJ Connector</td>
<td>A multi-modal type connector. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>ST Feedthru</td>
<td>A shielded bayonet type feedthru. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>SC Feedthru</td>
<td>A push/pull type feedthru. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>FDDI Feedthru</td>
<td>A push/pull type feedthru. This connector is one of the most popular styles.</td>
</tr>
<tr>
<td>FC Feedthru</td>
<td>A connector type feedthru. This connector is one of the most popular styles.</td>
</tr>
</tbody>
</table>

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
The backbone multi-mode fibre optic cabling and conduit system between buildings shall be installed in a star topology from the Central equipment room to each local control area. The system shall be installed in such a way that a failure of a single cable shall not affect the operation and communications to other local areas from the Central Control Room.

1.1.1.9.1 OTHER SECURITY SERVICES FIBRE OPTIC REQUIREMENTS

Fibre optic cable shall be supplied and installed in the quantities and location indicated on the drawings for other elements of the security services installation as part of these works. These requirements are generally to remote CCTV and SMS locations and will generally require conventional tight buffered 80/125 multi-mode fibre-optic cable approved for in-ground installation in sealed in-ground conduit.

1.1.1.9.2 FIBRE OPTIC GENERAL

A fibre-optic cabling network shall be provided for the connection and integration of various services to all nominated buildings. The fibre optic cable for the security services installation forms part of this contract.

The dedicated security services fibre optic cables will be terminated as part of this contract at 19” equipment racks or equipment cabinet installed in the nominated buildings.

Patch fibers to extend the fibre cable from the equipment racks or cabinets at which the cable terminates to the security equipment racks shall be provided in a ST terminal array. Optical fibre fly-leads to connect security services equipment to this point shall be supplied and installed by the security services sub-contractor.

The nominated security services element of the fibre optic cable network shall be utilized solely for the distribution of all security services.

Leave an excess of three meters of fibre neatly coiled up at each termination to provide spare fibre for any re-termination work in the future.

Cables shall be broken out into an approved Fibre Optic Termination Panel (FOTP) as per the cable manufacturer’s specifications.

Optical pigtails shall be terminated on the trunk side of the patch panel, using ST Bulkheads.

1.1.1.9.3 FIBRE OPTIC PATCH PANEL (FOPP)

All FOPPs shall be 19” rack mountable, or mounted in a suitable enclosure in the equipment racks and equipment enclosures. Security services FOPPs in buildings will be supplied and installed as part of this contract.

All FOPPs shall provide for fibre optic termination and any through splicing and/or patching facility.

The FOPPs shall be an industry standard type and shall consist of:

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
(a) Fibre optic patch panel capable of terminating "ST" style bulkheads.

(b) The FOPP shall have twenty four (24) "ST" style bulkhead terminations. If more terminations are required for a cable, multiple FOPPs shall be used to terminate the cable.

(c) Splice organiser cassettes shall be provided to accommodate all the splices as shown in the picture above.

(d) PVC gland entries shall be provided for up to six (6) incoming optical fibre cables.

(e) An approved strain relief fixing shall be provided for each central strength member.

(f) Cable strain relief/management provision shall be provided for internal and outgoing optic patch cables.

All FOPPs shall be accompanied by a 1U 19” Blank Panel (See Section 1.1.8.7) and a 1U Brush Panel (See Section 1.1.8.1) to ensure the correct bending radius of the fibre and a neat installation. The following pictures illustrate the method of installation as well as the neatness expected.

1.1.9.4 FIBRE OPTIC SPLICE BOX (FOSB)
All FOSBs shall be IP67 waterproof enclosures. Security Services FOSBs for the perimeter fence or other places where they are needed shall be supplied and installed as part of the Fibre Optic Sub-Contract.

All FOSBs shall provide for fibre optic termination and any through splicing.

**The FOSBs shall be an industry standard type and shall consist of:**

(a) A “York Box” capable of terminating an "ST" style bulkhead.
(b) The standard FOPP shall have one (1) "ST" style bulkhead termination. Non standard FOPP having two (2) "ST" style bulkhead terminations can also be used in applications where more than one fibre have to be broken out of the core. These special cases will be indicated on the Engineers Drawings.
(c) Splice organiser cassettes shall be provided to accommodate all the splices as shown in the picture above.
(d) PVC gland entries shall be provided for up to two (2) incoming optical fibre cables.
(e) An approved strain relief fixing shall be provided for each central strength member.
(f) Cable strain relief/management provision shall be provided for internal and outgoing optic patch cables.

### 1.1.1.9.5 FIBRE OPTIC CABLE AND EQUIPMENT TESTING

<table>
<thead>
<tr>
<th>FIBRE AND TRANSMITTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIBRE OPTIC VIDEO TRANSMITTER</td>
</tr>
<tr>
<td>RG-58U</td>
</tr>
<tr>
<td>POWER METER LIGHT SOURCE READING - LAUNCH POWER</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RECEIVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>MULTIMODE FIBRE</td>
</tr>
<tr>
<td>FIBRE OPTIC VIDEO RECEIVER</td>
</tr>
<tr>
<td>POWER METER LIGHT SOURCE READING - POWER OUTPUT</td>
</tr>
</tbody>
</table>

Figure 1 - Example of the required measurements to be done on fibre optic cabling and equipment

**The following measurements shall be done on all fibre optic cabling and equipment installed as part of this contract:**

(a) Launch power of the Fibre Optic Transmitter as measured with a Power Meter Light Source.
(b) An OTDR reading (Printout from the machine) for the stretch of fibre.
(c) Receive power on the fibre as measured with a Power Meter Light Source.
(d) The Power Output of the Fibre Optic Receiver as measured with a Power Meter Light Source.
For the Fibre and the Transmitter the data shall be supplied in the following format:

<table>
<thead>
<tr>
<th>Transmitter No.</th>
<th>Serial No.</th>
<th>Fibre No.</th>
<th>Launch Power (dB)</th>
<th>Receive Power (dB)</th>
<th>OTDR Reading (dB)</th>
<th>Difference (dB)</th>
<th>Reason for the Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For the receiver the data shall be supplied in the following format:

<table>
<thead>
<tr>
<th>Receiver No.</th>
<th>Serial No.</th>
<th>Fibre No.</th>
<th>Output Power (dB)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.1.1.9.6 SPIDER DIAGRAMS

Spider Diagrams as shown in the picture below shall be required for every fibre installed on site. The colour codes of the fibre as well as the linking shall be shown in the diagram.

Figure 2 - Example of Fibre Spider Diagram
1.1.2 EARTHING SPECIFICATION

The Earthing connection to the Security Equipment shall be no more than a 1Ω connection. The Earthing shall be done from a single (SPUR Distribution Point) point to each part of the security installation e.g. Equipment/Wiring Closets, Service and Central Equipment Locations etc.

No daisy chaining of the Earthing connection shall be allowed, except as described in the section on high-rise buildings. The reticulation for the earth connection shall be done with no less than 70 mm² Green Isolated Copper Conductor (GICC). The same spur point shall be connected to the Electrical Earth. The connection to the Electrical Earth can be done with Bare Copper Conductor (BCC) with a cross sectional area of no less than 70 mm².

The copper conductors shall be terminated in a lug which shall be bolted to the Earthing bar. The Earthing bar shall not be smaller than 6 mm x 50 mm x 300 mm. No more than 1 conductor per lug and no more than 1 lug per terminal point on the earthing bar will be tolerated. The lugs shall be crimped or CAD welded to the conductor and shall be inspected by the engineer prior to acceptance. The Security and Electrical Earths shall be run in separate conduits and be separated by no less than 1 m. The Earthing conductors may cross each other and any other electrical cable at a 90° angle.

All Earthing bars, screws, lugs & isolators shall comply with the SABS 0142 Wiring Code, SABS 03 Earthing Specification & all relevant IEC standards.

The following diagrams illustrate typical earthing installations:

![Diagram of Earthing Installation](image)

1.1.3 LIGHTNING AND SURGE PROTECTION SPECIFICATION
1.1.3.1 GENERAL

The contractor shall provide and install all the necessary Transient Voltage Surge Suppression (TVSS) devices, for the protection of the electrical/electronic control equipment, communication and data lines. TVSS devices shall protect all AC and DC circuits from the effect of lightning induced over voltages, internally generated transients and utility switching transients.

Lightning protection will be required on the incoming power supply to the security equipment and shall be done at the single point where the supply enters the building. Lightning protection shall be installed from Live to Earth (L-E), Neutral to Earth (N-E) and from Live to Neutral (L-N) on a single phase supply. If a 3 phase supply is used lightning protection shall be required on each phase individually (L1-E, L2-E, L3-E & N-E). If the same supply is reticulated to another building additional lightning protection shall be required where it enters the next building. The protection shall be as described above.

1.1.3.2 TVSS TECHNOLOGY – AC POWER APPLICATIONS

(a) The primary suppression path shall be pure silicon avalanche diodes
(b) Silicon avalanche diodes must be bi-polar, of grade A, + 5 % tolerance
(c) Surge suppression devices shall provide ‘power on’ and ‘failure’ indication. An optional remote status capability for indication of primary suppression path failure shall be available.
(d) All AC TVSS devices shall be UL listed and bear the UL label on each component. All AC TVSS devices shall be tested in accordance with the ANSI/IEEE testing standard.
(e) Gas tubes, Selenium plates, MOV or Hybrid type suppressors will not be accepted
(f) AC power protection units shall be in accordance with the specifications and regulations as proposed by the IEC.
(g) AC protection components shall be installed on the supply side of the local control room UPS.

1.1.3.3 TVSS TECHNOLOGY – DC POWER APPLICATIONS

(a) The primary suppression path shall be pure silicon avalanche diodes
(b) Silicon avalanche diodes must be bi-polar, A grade, + 5% tolerance.
(c) Surge suppression devices shall operate in parallel to the protected circuit shall not employing switching components and have no series resistance.
(d) Surge suppression devices shall provide a minimum of 5 joules or silicon avalanche diode per line, not per device.
(e) Initial clamping voltage shall not exceed the signal line voltage by more than 25% unless recommended by the security equipment manufacturer.
(f) Gas tubes, selenium plates, MOV or hybrid type suppressors will not be accepted
(g) Coaxial transient suppressor: TCS-CP 1 or approved equal.

1.1.3.4 APPLICATION

(a) Install TVSS devices on all AC supply lines and communication lines to protect against surges induced on all control lines, sensors, data lines and cables, which enter and exit buildings.
(b) Communication protection devices shall be mounted in IP54 enclosures with all wiring in the enclosure to be kept in plastic wiring troughs.
(c) The incoming cables shall be separated from outgoing cables.
(d) There shall be an earth bar in the lower corner of each enclosure and shall be sized to accept a 16mm square BCW. The Bare Copper Wire shall be terminated to the nearest earth mat.
(e) AC protection devices can be located in the equipment cabinet and must be installed prior to any distribution (i.e. multi-outlets).
(f) The contractor shall ensure that lightning surges of 10Ka @ 8/2 can be safely accommodated by the TVSS devices installed without damaging the surge suppression equipment permanently.
1.1.4 EQUIPMENT FIXING REQUIREMENTS

Under no circumstances shall double sided tape be used anywhere on this installation for whatever purpose.

1.1.4.1 SPECIFIC SURFACE REQUIREMENTS

1.1.4.1.1 DRYWALL

Dry wall plugs, Toggle Bolt anchors (Butterfly nuts) or Superfast™ Toggle anchors may be used to fix equipment, conduit or trunking.

1.1.4.1.2 BRICK WALLS

HILTI, Fisher, UPAT or RAWL type plugs are acceptable for fixing equipment, conduit or trunking.

1.1.4.1.3 CONCRETE

HILTI gun, RAWL bolts or chemical bolts are an acceptable means of fixing equipment, conduit or trunking.

1.1.4.1.4 CEILINGS

For suspended ceilings, Toggle Bolt anchors (Butterfly nuts) or Superfast™ Toggle anchors are an acceptable means of fixing equipment, conduit or trunking. Drywall screws will also be accepted if they are screwed directly into the support struts.

For normal ceilings Toggle Bolt anchors (Butterfly nuts) or Superfast™ Toggle anchors are an acceptable means of fixing equipment, conduit or trunking.

1.1.4.1.5 STEEL

**Up to 3mm:** Self tapping screw with drill, a self tapping screw or aluminium pop rivets (except for door hinges) are an acceptable means of fixing equipment, conduit or trunking.
Above 3mm: bolts and nuts are an acceptable means of fixing equipment, conduit or trunking.

1.1.4.1.6 WOOD

Drywall screws are an acceptable means of fixing equipment, conduit or trunking.

1.1.4.1.7 ALUMINIUM

A self tapping screw or aluminium pop rivets (except for door hinges) are an acceptable means of fixing equipment, conduit or trunking.

1.1.4.2 SPECIFIC EQUIPMENT INSTRUCTIONS

When attaching any of the following equipment, follow the guidelines of the surface the equipment is being attached to, unless otherwise stated.

1.1.4.2.1 ALARM WIRE

A glue gun or contact adhesive shall be used instead of the surface requirements as specified in section 1.1.6.1 of this document.

1.1.4.2.2 TRUNKING

Trunking shall be fixed at minimum intervals of 1 m.

1.1.4.2.3 CONDUITS

Raised aluminium saddles shall be used if the conduit is installed surface mount.

1.1.4.3 TAMPERPROOF SCREWS, BOLTS AND NUTS

All security equipment shall be installed with tamperproof fixings.

The following types of tamperproof fixings are acceptable:

Snake Eyes® Spanner Bolts & Screws.

Philips Pin-Head Bolts & Screws.

Allan Key Pin-Head Bolts & Screws.

Torx® Pin-Head Bolts, Screws & Self Drilling Screws.

Tri-Wing® Bolts & Screws.

OPSIT™ Reverse Thread Screws.
Tamperproof fixings shall comply with the following specifications:

(a) Material:
   - Screws & Bolts – 18-8 Stainless Steel.
   - Nuts – Zinc alloy or Aluminium for breakaway nuts.
(b) Metric or Imperial.
(c) Matching driver bit required.

Two sets of driver bits for all tamperproof fixings used on site shall be supplied to the CLIENT at site handover.
1.1.5 SIGNS, MARKERS, NAMEPLATES AND TAGS

Signs, Markers Nameplates and Tags shall comply with the following specifications:

(a) Signs, Markers Nameplates and Tags shall be totally:
   • UV-resistant;
   • Fade-resistant;
   • and Corrosion resistant.
(b) Shall have a minimum life expectancy of 10 years.
(c) Shall not be damaged by any commercially available solvent.

1.1.5.1 CABLE TAGS

(a) Cable tags shall be provided in accordance with SABS.

1.1.5.1.1 GENERAL

(a) Generally all cables shall be allocated an identifiable and unique cable number. All cables including patch leads shall be clearly labeled. Labels shall be affixed within 250 mm of each termination.
(b) Cables shall be fitted with tags at the following points:
   • On the cable sheath next to the gland at each end.
   • In cable pits.
   • At any additional point on the cable sheath (or around the core bunch) where the preceding requirements are not readily traceable from the core terminations.
   • Any inspection box or round box cover.
(c) Cable identification tags shall be orientated uniformly to read:
   • left to right from the logical viewing point horizontally.
   • from bottom to top viewed from the right where installed vertically.
(d) Duplication of cabling and equipment identities shall be avoided at all cost.

1.1.5.1.2 CABLE TAGGING REQUIREMENTS

For the labeling of cables any one of the following methods is acceptable:

(a) Cable-Tie Markers:
1.1.5.2 NAMEPLATES

Nameplates shall comply with the following specifications:

In order for the officers inside the compound to easily identify equipment locations a 250 mm X 200 mm sign shall be installed on each field cabinet. The sign shall face the inside of the compound and be installed on the door of the field cabinet.

(a) Precision engraved letters and numbers with uniform margins.
(b) Character sizes shall be a minimum of 50 mm high.
(c) Indoor:
   • Shall be phonemic, two colour laminated stock;
   • Minimum Thickness: 2 mm;
   • Machine engraved to expose the core colour (white).
(d) Outdoor:
   • Shall be standard aluminium alloy plate stock;
   • 1 mm;
   • Engraved areas shall be enamel filled (black) or background enamelled with natural aluminium engraved characters.
(e) All nameplates shall be permanently attached.

1.1.5.3 ZONE IDENTIFICATION MARKERS
Zone Identification Markers shall comply with the following specifications:

In order for the officers inside the compound to easily identify zone locations, zone identification signs shall be installed at the top of a sensor post at 9 m intervals. The sign shall have a size of 250 mm X 200 mm and shall face the inside of the compound at a height of 1.5 m.

(a) All zones shall be identified by zone number.
(b) Reflective white numbers on a dark blue background shall be used.
(c) The sign shall have sufficient securing holes to prevent movement and/or theft.
(d) Signs shall be supplied with sign ties.
(e) The lettering on the sign shall be large enough to read from a distance of at least 10 m away by a person with 20/20 vision.

In order for the perimeter patrol officer to easily identify zone locations, at the beginning and end of each zone a 500mm x 250mm sign shall be installed. The sign shall face the inside of the compound and be installed at a height of 1.5 m approximately 1 m from the beginning or end of the zone.

(a) All zones shall be identified by zone number.
(b) Black numbers on a reflective yellow background shall be used.
(c) The sign shall have sufficient securing holes to prevent movement and theft.
(d) Signs shall be supplied with sign ties.
(e) The lettering on the sign shall be large enough to read from a distance of at least 10 m away by a person with 20/20 vision.

1.1.5.4 ELECTRIFIED FENCE WARNING SIGNS

Warning Signs shall be fixed to the fence at a height of approximately 1.5 m. These signs shall be installed every 9 m along with the zone markers.

The Electrified Fence Warning Signs shall comply with the following specifications:

(a) Comply with all legal requirements to warn the public.
(b) The sign shall have sufficient securing holes to prevent movement and theft.
(c) Signs shall be supplied with sign ties.
(d) Shall be large enough to read from a distance of at least 10 m away by a person with 20/20 vision.

1.1.6 19” RACKS

1.1.6.1 GENERAL

To save space inside the equipment room, and to keep the installation neat, equipment shall be installed in the 19” racks.

1.1.6.2 INSTALLATION REQUIREMENTS AND LAYOUT
The cabinets shall be lockable and the key will be controlled by the Client.

The racks shall comply with the following specifications:

(a) Fixed 19” installation front and rear, for components in accordance with IEC 297-3.
(b) Flexible mounting for components with T-slot mountings.
(c) Cable entry via the plinth and top cover.
(d) Heat dissipation discharge via a vent lid or fan top.
(e) Door open angle 180°.
(f) Cross connecting jumper space shall be at least 120mm to the front and rear.
(g) An IP40 protection rating.
(h) Load rating shall be 500kg, static.
(i) Height : 15U, 20U, 24U, 33U, 38U, 42U or 47U (1U = 44.45mm).
(j) Width : Inside – 482.6mm (19") / Outside – 600mm.
(k) Depth : 600mm or 800mm.
(l) Tests :
   • Earthing according to VDE 0100 T 540.
   • Seismic test according to MIL-STD 810E.
   • IP test according to DIN 40 050 / IEC 529.
(m) Other Standards : EN60950 and EN60529.
(n) Finish :
   • Rear Panel & Basic Rack – sheet steel, zinc passivated, powder coated.
   • Covers (Removable) – sheet steel, zinc passivated, powder-coated.
   • Glass Door Infill – single safety glass panel, 4mm.
   • Multifunctional Struts – sheet steel, zinc passivated.
   • Colour : Door Trim – RAL9011, black.
   • Visible Cover Surfaces – RAL7035, light grey.
(o) Supply Schedule :
   • 1 X Basic Rack.
   • 2 X 19” Aluminium extrusions with T-slot and increment slide for spring nut M5.
   • 2 X Multifunctional struts for cable clamping and universal mounting options.
   • 1 X Top cover with fan cover. Minimum of two (2) fans installed with a rating of 108m3/h per fan.
   • 1 X Front single door, single safety glass panel, with handle and cylinder lock.
   • 1 X Rear single door, sheet steel, with handle and cylinder lock.
   • 2 X Side panels with quick-release fasteners.
   • 1 X Plinth for cable routing, side and rear, with heavy duty castors (Two of the castors to be of the lock type).
   • 2 X Side plinth trims, closed.
• 2 X Plinth trims for front and rear side, with ventilation slots and fixing for filter mats. Filter mats to be included.
• 1 X Earthing set, complete [VDE 0100].

(p) To be supplied fully assembled.

1.1.7 WALL MOUNNT 19” RACKS

The racks shall comply with the following specifications:

(a) Fixed 19” installation front, for components in accordance with IEC 297-3.
(b) Flexible mounting for components with T-slot mountings.
(c) Covers above and below with brush strips for cable entry and with side vent slots.
(d) Heat dissipation discharge via a vent lid or fan top.
(e) Door open angle 180°.
(f) Cross connecting jumper space shall be at least 100mm to the front and 50mm to the sides.
(g) An IP20 protection rating.
(h) Load rating shall be 50kg, static.
(i) Height : 6U, 9U, 12U, 15U, 18U or 21U (1U = 44.45mm).
(j) Width : Inside – 482.6mm (19") / Outside – 600mm.
(k) Depth : 400mm, 500mm or 600mm.
(l) Tests :
  • Earthing according to VDE 0100 T 540.
  • Seismic test according to MIL-STD 810E.
  • IP test according to DIN 40 050 / IEC 529.
(m) Other Standards : EN60950 and EN60529.
(n) Finish :
  • Basic Rack – extruded aluminium, polished or powder-coated.
  • Corner Connectors – die cast aluminium, polished or powder-coated.
  • Covers – sheet steel, zinc passivated, powder-coated, textured.
  • Glass Door In fills – single safety glass panel, 4mm.
  • Multifunctional Struts – sheet steel, zinc passivated.
(o) Colour :
  • Door Trim – RAL9011, black.
  • Visible Cover Surfaces – RAL7035, light grey.
(p) Supply Schedule :
  • 1 X Basic wall-standing enclosure.
  • 2 X 19” Vertical extrusions.
  • 2 X Cable clamping rail.
• 1 X Top fan cover. Minimum of two (2) fans installed with a rating of 108m³/h per fan.
• 1 X Earthing set, complete [VDE 0100].
• All mounting materials.

(q) To be supplied fully assembled.

1.1.8 19” RACK ACCESSORIES

1.1.8.1 BRUSH PANELS

The brush panels shall compl[y with the following specifications:

(a) Mountable in racks with a fixed 19” installation front or rear.
(b) Height : 1U (1U = 44.45mm).
(c) Material : 1.5mm sheet steel or die cast aluminium.
(d) Colour / Finish : Powder-coated, RAL9011, black.
(e) Supply Schedule :
   • 1 X 19” Brush panel.
   • All mounting materials.

Brush panels shall be installed in 19” racks to neaten the cables.
Brush panels shall be installed above and below all BNC and Fibre patch panels.

1.1.8.2 CABLE ROUTING PANELS
The cable routing panels shall comply with the following specifications:

(a) Mountable in racks with a fixed 19” installation front or rear.
(b) Height : 1U (1U = 44.45mm).
(c) Material :
   - Front Panel – 1.5mm sheet steel.
   - Cable Routers – 55mm X 22mm plastic or 95mm X 32mm steel.
(d) Colour / Finish : Front Panel – powder-coated, textured, RAL7035, light grey.
(e) Supply Schedule :
   - 1 X 19” Front panel.
   - 5 X Cable routers.
   - All mounting materials.
   - To be supplied fully assembled.

Cable routers shall be installed in 19” racks to neaten the cables. This shall be done at the engineer’s discretion.

1.1.8.3 CABLE ROUTING RINGS

The cable routing rings shall comply with the following specifications:

(a) Mountable on the T-slots and vertical extrusions.
(b) The installation position shall be selectable.
(c) Material : Cable Routing Rings – 95mm X 32mm steel.
(d) Colour / Finish : Powder-coated, textured, RAL7035, light grey.
(e) Supply Schedule :
   - 5 X Cable routing rings.
   - All mounting materials.

Cable routing rings shall be installed in 19” racks to neaten the cables. This shall be done at the engineer’s discretion.

1.1.8.4 CABLE JUMPERING BRACKET
The jumpering brackets shall comply with the following specifications:

(a) Mountable on the T-slots and vertical extrusions.
(b) The installation position shall be selectable.
(c) Material:
   - Square Cable Jumpering Brackets – 86mm X 86mm steel.
   - Rectangular Cable Jumpering Brackets – 24mm X 288mm steel or 38mm X 288mm steel.
(d) Colour / Finish:
   - Zinc Passivated or
   - Powder-coated, textured, RAL7035, light grey.
(e) Supply Schedule:
   - 1 X Cable Jumpering Bracket.
   - All mounting materials.

Cable jumpering brackets shall be installed in 19” racks to neaten the cables. This shall be done at the engineer’s discretion.

1.1.8.5 SHELF

The shelves shall comply with the following specifications:

(a) Mountable in racks with a fixed 19” installation front.
(b) Material shall be 1.5mm sheet steel.
(c) Depth: 250mm, 320mm, 450mm or 500mm.
(d) Colour / Finish: Powder-coated, textured, RAL7035, light grey.
(e) Load rating shall be 20kg, static.
(f) Supply Schedule:
   - 1 X Shelf, fixed.
   - All mounting materials.

Shelves shall be used to install equipment without 19” rack mounting options in 19” racks.

1.1.8.6 PULL-OUT SHELF

The shelves shall comply with the following specifications:

(a) Mountable in racks with a fixed 19” installation front.
(b) Supplied with a handle.
(c) Material:
   - Shelf – 1.0mm sheet steel.
   - Telescopic Slides – cold rolled steel.
(d) Depth: 450mm or 600mm.
(e) Colour / Finish : Powder-coated, textured, RAL7035, light grey.
(f) Load rating shall be 20kg, static.
(g) Supply Schedule :
   - 1 X Shelf, fixed.
   - X Telescopic Slides.
   - All mounting materials.
(h) To be supplied fully assembled.

Pull-Out Shelves shall be used to place keyboards beneath where PCs is installed in 19” racks.

1.1.8.7 BLANK PANELS

The blank panels shall comply with the following specifications :

(a) Mountable in racks with a fixed 19” installation front or rear.
(b) Height : 1U, 2U, 3U, 6U or 9U (1U = 44.45mm).
(c) Material : 1.5mm sheet steel.
(d) Colour / Finish : Powder-coated, textured, RAL7035, light grey.
(e) Supply Schedule :
   - 1 X Blank panel.
   - All mounting materials.

All open areas on the front of a supplied 19” rack are to be blanked off with the appropriate blanking panels.

1.1.8.8 BRUSH COVERS

The brush covers shall comply with the following specifications :

(a) Mountable in the bottom of racks for cable entry.
(b) Material : 1.5mm sheet steel.
(c) Colour / Finish : Powder-coated, textured, RAL7035, light grey.
(d) Supply Schedule :
   - 1 X Brush Cover.
   - All mounting materials.

The 19” racks shall be fitted with these brush cover strips and sufficient brush covers shall be installed to enable neat cabling and proper bending radii of cabling in the rack.

1.1.8.9 MOUNTING MATERIALS
All mounting materials in the above 19” rack section refers to:

(a) M6 cage nuts.
   - Philips or Slotted pan head screws M6 X 12mm or M6 X 16mm depending on the
     thickness of the item being fixed.
(b) A Rosette/Locating washer for each screw.

Every item installed in the 19” rack will be supplied with the necessary number of
mounting materials, i.e. if the item has 4 mounting holes, 4 of each of the above items
shall be supplied.

1.1.8.10 POWER STRIPS (MULTI-PLUGS)

The power strips shall comply with the following specifications:

(a) Versatile all-metal cabinet with detachable mounting flanges allows rack mount, wall mount,
    under counter and other creative mounting options.
(b) 6, 8, 12 or 16 Dedicated Socket Outlets (RED).
(c) 15, 20 and 30 Amp UL and CUL listed.
(d) 4-way Universal Mounting.
(e) Resetable circuit breaker with surge protection.
(f) The outlets shall be generously spaced to improve cable management.
(g) Available in 19” Rack Mount, 28”, 40” and 66” Lengths for Vertical or Horizontal Cabinet and
    Rack Mounting.
(h) An IP40 protection rating.

1.1.8.10.1 19” HORIZONTAL MOUNTING OPTION

(a) Fixed 19” installation front or rear in accordance with IEC 297-3.
(b) Height : Maximum of 2U (1U = 44.45mm).
(c) Width : 482.6mm (19”)
(d) Depth : Maximum of 100mm.
(e) Finish :
   - Extruded aluminium, polished or powder-coated.
   - Covers – sheet steel, zinc passivated, powder-coated, textured.
(f) Colour : Outer Surfaces – RAL7035, light grey.

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
(g) Supply Schedule:
   - 1 X Surge Protected Power Strip with a power cord that is at least 2m long.

(h) To be supplied fully assembled.

1.1.8.10.2 19" VERTICAL MOUNTING OPTION

(a) Width : Maximum of 100mm.
(b) Depth : Maximum of 100mm.
(c) Finish :
(d) Extruded aluminium, polished or powder-coated.
(e) Covers – sheet steel, zinc passivated, powder-coated, textured.
(f) Colour : Outer Surfaces – RAL7035, light grey.
(g) Supply Schedule:
   - 1 X Surge Protected Power Strip with a power cord that is at least 2m long.

(h) To be supplied fully assembled.

The 19" racks shall be fitted with these multi-plug strips and there shall be one plug per piece of equipment installed in the rack.

1.2 COMPUTER HARDWARE

1.2.1 OPERATOR WORKSTATIONS, CARD PRINTING STATIONS AND SERVERS

Operator Workstations and Servers shall be standard Intel® Pentium® based computer systems employing the relevant 32-bit or 64-bit edition of Microsoft® Windows 7 or Windows 8.1, Windows Server 2012 or later where applicable.

1.2.1.1 TORTURE / STRESS TESTING HARDWARE

A program like Win Prime 95, that is freely available on the internet, shall be used to stress test the computers before delivery. The torture test shall run for at least 12 hours. Additionally a few passes of the latest version of a ram stress test like Memtest86 shall also be run.

A test report of the stress test shall be supplied with each PC or Server.

1.2.1.2 OPERATOR WORKSTATIONS

The PC shall comply with the following minimum specifications:

(a) One Intel® Xeon® Processor E5-2650 v3 (10C, 2.3GHz, 25M, 105W);
(b) 32G 2133MHz DDR4 (4x8GB) RDIMM ECC;
(c) 2.5 inch 256GB SATA SSD for Operating System;
(d) 3.5 inch 1TB SATA 7.2k RPM HDD for Data;
(e) 16X DVD ROM Drive;
(f) 4 X USB 3.0 Ports (Backwards compatible with USB 2.0, USB 1.1 and USB 1.0);
(g) 10/100/1000 Ethernet LAN Card;
(h) Keyboard and Mouse (See Section 1.1.1.3);
(i) Dual 2 GB NVIDIA QUADRO K620 (2cards w/ 1DP & 1DVI-I each) (2DP-DVI & 2DVI-VGA adapter).
(j) 500 Watt PC Power Supply;
(k) Windows 7, 8.1 Professional or later 64 bit preloaded (licence key supplied by University);
(l) All other software systems necessary to make the Workstation fully operational;
(m) All driver and OS disks to be supplied;
(n) A 12 hour burn in and stress test certificate shall be supplied with the computer.
(o) **Support**: 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

### 1.2.1.3 CARD PRINTING / TAKE-ON STATIONS

The PC shall comply with the following minimum specifications:

(a) One Intel® Core™ i7 (4770S);
(b) 16 GB (4x4GB) 1333MHz DDR3 ECC UDIMM;
(c) 2.5 inch 256GB SATA SSD for Operating System;
(d) 3.5 inch 1TB SATA 7.2k RPM HDD for Data;
(e) 16X DVD ROM Drive;
(f) 4 X USB 3.0 Ports (Backwards compatible with USB 2.0, USB 1.1 and USB 1.0);
(g) 10/100/1000 Ethernet LAN Card;
(h) Keyboard and Mouse (See Section 1.1.1.3);
(i) Single 1 GB NVIDIA Quadro 600 (1card w/ 1DP & 1DVI-I each) (1DP-DVI & 1DVI-VGA adapter).
(j) 500 Watt PC Power Supply;
(k) Windows 7, 8.1 Professional or later 64 bit preloaded;
(l) All other software systems necessary to make the Workstation fully operational;
(m) All driver and OS disks to be supplied;
(n) A 12 hour burn in and stress test certificate shall be supplied with the computer.
(o) **Support**: 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

### 1.2.2 SERVERS

#### 1.2.2.1 MEDIUM INSTALLATION CCTV RECORDER AND VIRTUAL SERVER

The Medium Installation CCTV Recorder and Virtual Server shall be a Data-Centre-In-A-Box iSCSI and VM Hypervisor Storage Appliance ideal for up to 512 Cameras with a reasonable Long Retention Time. The Server will be capable of providing at least 8 x VMs for NVR and/or VMS applications, Physical Security Information Management (PSIM), Security Management System (SMS), Video Management System (VMS), Intrusion Detection System (IDMS) and IP Intercom Server (IP PBX).

The Medium Installation CCTV Recorder and Virtual Server shall comply with the following minimum specifications:

Supply Characteristics:
- Nominal Voltage: 220 VAC;
- Voltage Range: 200 VAC – 240 VAC;
- Maximum Consumption:
  - Operation: 975W.
- Operating Frequency: 47-63 Hz.
- Average Cooling:
- 2350 BTU/hr.
- **Maximum Weight:**
  - 65 kg (with all Hard Drives installed)

**Communication:**
- **Protocol:** GE Ethernet:
  - Number of Ports: 10;
  - Minimum Communications Distance: 90 m.
- **Protocol:** 10GE Fibre Channel:
  - Number of Ports: 10;

**Operating Environmental Conditions:**
- Temperature Range: 10°C – 35°C;
- Relative Humidity: 5% – 95% Non-Condensing Relative Humidity;

**Indication:**
- 2-LED Module Status Display:
  - Power;
  - HDD.

**No of CPU Sockets:**
- 2;

**Processors:**
- Intel Xeon Processor:
- No. of Cores: 6 to 18;

**Storage:**
- Hard Drives:
  - Up to 24 x SATA / SAS HDDs dedicated for CCTV Footage.
- Scalable Storage Size:
  - from 2 TB to 192 TB.

**Cache:**
- Size: 128 GB.

**Memory:**
- 64 GB RAM;

**Recommended Maximum No. of Cameras:**
- 512.

**Virtualization Hypervisor:**
- No. of VMs for NVR / VMS Applications:
  - 8.
- VMs Used For:
  - Physical Security Information Management (PSIM);
  - Security Management System (SMS);
  - Video Management System (VMS);
  - Intrusion Detection System (IDMS);
  - and IP Intercom Server (IP PBX).

**Fault Tolerance:**
- Support RAID 5/6/10 with ZFS for Video Recordings;
- Support RAID 5/6/10 for the Operating System.

**Mounting Options:**
- 19” Rack Mount on Rails.

**Enclosure:**
- Colour:
  - RAL9011, black;
- Typical Dimensions:
  - 4U Rack Mount;
  - 698mm x 432mm x 176mm Zinc Passivated, Powder Coated Metal Enclosure.

**Certifications:**
- UL, CE, CUL, FCC

**Features:**

---

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
• Native Support of iSCSI Protocol;
• Guarantee of QoS with Direct Access to PCIe Buses;
• High Performance, with Cache Tiering using Dedicated Solid State Hard Drives;
• Redundant, Hot Swappable Hardware Components for Maximum Uptime.

If equivalent hardware is proposed then the supplier must be able to demonstrate compatibility of software as described in Section 8.3.3.

All software and operating systems necessary to make the Server fully operational;
All driver and OS disks to be supplied;
A 12 hour burn in and stress test certificate shall be supplied with the computer.

**Support** : 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

**Proprietary hardware platforms are not acceptable.**

### 1.2.2.2 LARGE INSTALLATION CCTV RECORDER AND VIRTUAL SERVER

The Large Installation CCTV Recorder and Virtual Server shall be a Data-Centre-In-A-Box iSCSI and VM Hypervisor Storage Appliance ideal for up to 512 Cameras with a reasonable Long Retention Time. The Server will be capable of providing at least 8 x VMs for NVR and/or VMS applications, Physical Security Information Management (PSIM), Security Management System (SMS), Video Management System (VMS), Intrusion Detection System (IDMS) and IP Intercom Server (IP PBX).

The Large Installation CCTV Recorder and Virtual Server shall comply with the following minimum specifications :

**Supply Characteristics** :
- Nominal Voltage : 220 VAC;
  - Voltage Range : 200 VAC – 240 VAC;
- Maximum Consumption :
  - Operation : 1100W.
- Operating Frequency :
  - 47-63 Hz.
- Average Cooling :
  - 3400 BTU/hr.
- Maximum Weight :
  - 105 kg (with all Hard Drives installed)

**Communication** :
- Protocol : GE Ethernet :
  - Number of Ports : 10;
  - Minimum Communications Distance : 90 m.
- Protocol : 10GE Fibre Channel :
  - Number of Ports : 10;

**Operating Environmental Conditions** :
- Temperature Range : 10°C – 35°C;
- Relative Humidity : 5% – 95% Non-Condensing Relative Humidity;

**Indication** :

• 2-LED Module Status Display:
  ▪ Power;
  ▪ HDD.
No of CPU Sockets:
• 2;
Processors:
• Intel Xeon Processor;
• No. of Cores: 6 to 18;
Storage:
• Hard Drives:
  ▪ Up to 48 x SATA / SAS HDDs dedicated for CCTV Footage.
• Scalable Storage Size:
  ▪ from 2 TB to 384 TB.
Cache:
• Size: 256 GB.
Memory:
• 64 GB RAM;
Recommended Maximum No. of Cameras:
• 512.
Virtualization Hypervisor:
• No. of VMs for NVR / VMS Applications:
  ▪ 8.
• VMs Used For:
  ▪ Physical Security Information Management (PSIM);
  ▪ Security Management System (SMS);
  ▪ Video Management System (VMS);
  ▪ Intrusion Detection System (IDMS);
  ▪ and IP Intercom Server (IP PBX).
Fault Tolerance:
• Support RAID 5/6/10 with ZFS for Video Recordings;
• Support RAID 5/6/10 for the Operating System.
Mounting Options:
• 19" Rack Mount on Rails.
Enclosure:
• Colour:
  ▪ RAL9011, black;
Typical Dimensions:
• 4U Rack Mount;
• 818mm x 447mm x 176mm Zinc Passivated, Powder Coated Metal Enclosure.
Certifications:
• UL, CE, CUL, FCC
Features:
• Native Support of iSCSI Protocol;
• Guarantee of QoS with Direct Access to PCIe Buses;
• High Performance, with Cache Tiering using Dedicated Solid State Hard Drives;
• Redundant, Hot Swappable Hardware Components for Maximum Uptime.
If equivalent hardware is proposed then the supplier must be able to demonstrate compatibility of software as described in Section 8.3.3.
All software and operating systems necessary to make the Server fully operational;
All driver and OS disks to be supplied;
A 12 hour burn in and stress test certificate shall be supplied with the computer.

Support: 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

Proprietary hardware platforms are not acceptable.
1.2.3 VIDEO WALL CONTROLLERS
1.2.3.1 MEDIUM VIDEO WALL CONTROLLER

This Type of Controller PC shall be installed to control video walls consisting of up to sixteen (16) large screens.

The PC shall comply with the following minimum specifications:

- Two Intel® Xeon® X5675 (Six Core, 3.06GHz, 12MB Cache, 6.4GT/s Intel® QPI);
- 64GB (8x8GB) 1333MHz DDR3 ECC RDIMM Requires 64 Bit OS;
- 2 X 300GB (15,000rpm) SAS Hard Drive;
- C21 All SAS Hard Drives, RAID 1 (Mirroring) for 2 Hard Drive;
- PERC6i Internal Controller Card PCIe x8;
- 16X DVD ROM Drive;
- 4 X USB 3.0 Ports (Backwards compatible with USB 2.0, USB 1.1 and USB 1.0);
- 10/100/1000 Ethernet LAN Card;
- Keyboard and Mouse (See Section 1.1.1.3);
- Dual 6 GB NVIDIA Quadro 6000 (2cards w/ 2DP & 1DVI-I each) (2DP-DVI adapter);
- Standard Base Full Tower (Vertical orientation);
- 750 Watt PC Power Supply;
- Windows 7 Professional 64 bit or later preloaded (licence key supplied by University);
- All software and operating systems necessary to make the Server fully operational;
- All driver and OS disks to be supplied;
- A 12 hour burn in and stress test certificate shall be supplied with the computer.

Support: 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

The PC shall be supplied complete with video wall control software.

1.2.4 MONITORS

All monitors shall be rated for 24/7/365 usage and the monitors to be used in a Screenwall shall automatically colour and brightness match.

1.2.4.1 MONITOR TYPE 1 – 23” LCD FLAT SCREEN

The monitors to be installed in the Security Control Room shall be full colour LCD type PC monitors with a direct composite video adapter built in. The screen edges shall not be more than 7mm wide. The screen shall be between 21” and 24” in size according to the engineer’s specifications for the job.

The monitor shall comply with the following minimum specifications:

- A 100 mm X 100 mm VESA Wall Mounting Bracket;
- A Built in USB 2.0 port;

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
Input Voltage : 90V – 264V @ 50 – 60Hz Universal Power Input;
Maximum Power Consumption : 220W;
Minimum Brightness : 500 cd/m²;
Contrast Ratio : 3000:1 or better;
Aspect Ratio : 16:9;
Display Colours : 16.7M;
Response Time : 10ms or better;
Minimum Resolution : 1920 X 1080;
Minimum Viewing Angle : 178° in both the Horizontal and Vertical Directions;
Interfaces :
- Inputs :
  - 15-pin D-Sub (VGA) connector;
  - HDMI connector;
  - PC Audio;
  - Component Audio;
  - Composite Audio;
  - RS232C.
- Outputs :
  - VGA (15pin D-Sub);
  - HDMI;
  - RS232C;
  - Speaker (Ready).
Environmental :
- Temperature Range : 0 – 40°C;
- Relative Humidity : 0 – 80% Non-Condensing;
On Screen Display;
Minimum Guaranteed Lifespan : 50,000 Hours.
Anti-Reflective Tempered Glass;
Automatic Brightness Control and Colour matching between Screens in a Screen Wall.
Maximum Bezel Size : 7 mm;
All software necessary to make the Monitor fully operational;
All driver disks to be supplied;
**Support** : 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

### 1.2.4.2 MONITOR TYPE 2 – 46” LCD FLAT SCREEN

The monitors to be installed in the Security Control Room shall be full colour LCD type PC monitors with a direct composite video adapter built in. The screen edges shall not be more than 7mm wide. The screen shall be 46” in size.

The monitor shall comply with the following minimum specifications:
Mounting: 400 mm X 200 mm 8 hole or 600 mm X 200 mm 8 hole VESA Wall Mounting Bracket;
Input Voltage: 90V – 264V @ 50 – 60Hz Universal Power Input;
Maximum Power Consumption: 220W;
Minimum Brightness: 500 cd/m2;
Contrast Ratio: 800:1 or better;
Aspect Ratio: 16:9;
Display Colours: 16.7M;
Response Time: 10ms or better;
Minimum Resolution: 1920 X 1080;
Minimum Viewing Angle: 178° in both the Horizontal and Vertical Directions;

Interfaces:
- Inputs:
  - VGA (15pin D-Sub);
  - HDMI;
  - Composite (BNC);
  - Component (BNC);
  - PC Audio;
  - Component Audio;
  - Composite Audio;
  - RS232C.
- Outputs:
  - VGA (15pin D-Sub);
  - HDMI;
  - Composite (BNC);
  - Component (BNC);
  - Component Audio;
  - Composite Audio;
  - RS232C;
  - Speaker (Ready).

Environmental:
- Temperature Range: 0 – 40°C;
- Relative Humidity: 0 – 80% Non-Condensing;
- On Screen Display;
- Minimum Guaranteed Lifespan: 50,000 Hours.
- Anti-Reflective Tempered Glass;
- Automatic Brightness Control and Colour matching between Screens in a Screen Wall.
- Maximum Bezel Size: 7 mm;
- All software necessary to make the Monitor fully operational;
- All driver disks to be supplied;

Support: 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

1.2.5 KEYBOARD & MOUSE

The Standard Keyboard shall comply with the following minimum specifications:

The keyboard shall be a standard soft touch PC-104 type keyboard;
Connection to the PC : USB;
Enhanced Function Keys.
Multimedia Controls.
All Software and Driver shall be included. The original manufacturers CDs shall be handed over to the CLIENT with the close out documentation.

The Standard Mouse shall comply with the following minimum specifications :

Connection to the PC : USB;
Optical or Laser Mouse with an 800 DPI resolution.
Internet Forward/Back.
Tilt Wheel plus Zoom.
Scroll Vertically, Pan Horizontally, and Zoom in and out of documents.

1.2.6 PRINTERS
1.2.6.1 REPORTS PRINTERS

The Report Printer shall comply with the following minimum specifications :

Printing System :
- Printing Technology : Network capable Laser Printer;
- Print Speed : Up to 25 pages per minute (ppm) monochrome A4 paper size;
- First Page Out Time : Under 10 seconds;
- Print Resolution : 1200 x 1200 dots per inch (dpi);
- Processor Speed : 400 MHz;
- Minimum Pages per month : 50,000;

Paper Handling / Media :
- Standard Paper Trays : 2;
- Maximum Number of Paper Trays : 3;
- Media types supported : Paper (plain, preprinted, letterhead, prepunched, bond, recycled, color, rough), transparencies, labels, envelopes, cardstock;
- Standard input capacity : 350 pages;
- Maximum input capacity : 850 pages;
- Standard output capacity : 250 pages;
- Maximum output capacity : 250 pages;
- Duplex Print Options : Automatic;
- Standard Media Sizes : A4, A5, B5 (JIS), letter, legal;
- Custom media sizes : Multipurpose Tray 1: 76 x 127 to 216 x 356 mm;
- Media weights by paper path :
  ▪ Multipurpose Tray 1: 60 to 200 g/m²;
  ▪ Tray 2/3: 60 to 120 g/m².

Memory / Print Languages :
- Standard Memory : 32 MB minimum;
- Maximum Memory : 288 MB;
- Memory Slots : 2 X 100-pin DDR DIMM slots (one open);
- Standard Printer Languages : HP PCL 6, HP PCL 5e, HP Postscript Level 3 Emulation, direct PDF printing v 1.3 (with at least 128 MB of printer memory);
- Minimum Typefaces : 80 font set (plus Greek, Hebrew, Cyrillic, Arabic);

Connectivity :

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
• 1 X IEEE 1284-B compliant parallel port;
• 1 X Hi-Speed USB port (compatible with USB 2.0 specifications);
• 1 X 10/100 Ethernet LAN port (optional extra).

Compatible Operating Systems :
• Microsoft® Windows® 7 or later.

Maximum Power Consumption :
• 625 watts (printing);
• 15 watts (standby);
• 10 watts (powersave);
• 0.5 watts (off);

Power Requirements :
• Input Voltage : 90 – 265 VAC;
• Frequency : 50-60 Hz ± 2%;

Minimum Temperature Ranges and Humidity :
• Operating : 15 – 30°C;
• Storage : -20 – 40°C;
• Relative Humidity : 20 – 80% Non-condensing RH;

Minimum Warranty : 1 year;

All software necessary to make the Printer fully operational;
All driver disks to be supplied;

Support : 3 Year Pro-Support and Next Business Day On-Site Service. If the Unit fails NBD On-Site fix, a loan Unit with same configuration to be put down. If Unit cannot be repaired in 7 working days the Loan Unit stays on site permanently.

1.3 POWER SUPPLIES

1.3.1 LARGE DC POWER SUPPLY UNITS WITH BATTERY BACK-UP

The power supply unit (PSU) shall be an AC in DC output type switch mode power supply (SMPS) with a built in battery back-up. Each unit shall consist of a maintenance free sealed lead acid battery together with an associated constant voltage current limited charger. Both units shall be housed in a single ventilated sheet steel enclosure. The units shall supply uninterrupted DC power to the load. Operation shall be such that power is supplied by the charger section when mains are present and by the battery during mains failure. The charger shall constitute a low ripple PSU in its own right. The PSU shall be able to supply the rated output current continuously without any de-rating.

The Power Supply shall comply with the following minimum specifications :

The AC input shall be fused.
The PSU shall have a green "Power ON" LED indicator.
Supply Characteristics :
• Nominal Voltage : 230 VAC.
• Voltage Range : 90 VAC – 265 VAC.
• Nominal Frequency : 50 Hz.
• Frequency Range : 45 Hz – 66 Hz.
• Notwithstanding any reference to 230 VAC supply, all equipment connected directly to the mains supply shall operate satisfactorily and without any reduction of its effective life under the voltage of the supply provided.
Operating Environmental Conditions :
• Temperature Range : -10°C – 70°C.
• Relative Humidity : 5% – 95% Non-condensing Relative Humidity.
• Minimum IP Rating : IP40.
Primary Suppression and Inrush Protection shall be compliant to :
• IEC 1000–4–4;
• IEC 1000–4–5;
• IEC 1000–4–11.
  Minimum Efficiency : 80%.
  The output voltage shall be filtered and regulated.
  The PSU shall have full short circuit protection.
  The PSU shall be fully protected against faulty or incorrect wiring and shall not in any way
  be damaged by such wiring.
  The following output ratings shall be available :
  • 12 VDC @ 3A;
  • 12 VDC @ 5A;
  • 12 VDC @ 10A;
  • 24 VDC @ 3A;
  • 24 VDC @ 5A;
  • 24 VDC @ 10A.
  The exact PSU to be used in the installation shall be indicated in the Bills of Quantities
  for the project.
  Maximum Output Ripple Voltage : 1% of the rated output.
  Voltage Regulation :
  • The output voltage shall be regulated within 1% of the rated output voltage.
  • If a load step (0% load – 100% of the rated load) is applied to the PSU the output
    voltage shall not over- or under-shoot by more than 5% and shall return to within 1%
    of the rated output voltage within 200 ms.
  The output current shall be limited to the rated current.
  Mounting Options :
  • DIN Rail Mounting;
  • Chassis Mounting;
  • Wall Mounting.
  Enclosure :
  • 2 mm sheet steel with sufficient ventilation, zinc passivated, powder-coated.
  • Colour : RAL9011, black.
  Mean Time Between Failures (MTBF) : 100,000 Hours.
  Battery Back-Up :
  • The battery shall be a maintenance free sealed lead type with sufficient capacity to
    supply the full rated load for one (1) hour after mains failure.
  EMC - European Union—EC
  • This equipment shall comply with the following requirements of the EMC Directive
    89/336/EEC:
    • EN55022 / CISPR22 (1985) Class A
    • EN50082-1 IEC801-2 (1991) 4 kV (Direct), 8 kV (Air)
    • IEC801-3 (1984) 3 V/m
    • IEC801-4 (1988) 1.0 kV Power Lines, 0.5 kV Signal Lines
    • EN61000-3-2/IEC1000-3-2(1994) Pass
  Safety
  • This equipment complies with the following requirements of the Low Voltage Directive
    73/23/EEC:
    • EN60950/IEC950 (1993)
  Sensors shall have complete electromagnetic and electrostatic protection against externally
  generated noise and the effects of devices such as fluorescent light fixtures, variable
  frequency motor controllers, cellular telephones, and electrical surges from other sources.
  Protection must meet the European Directive CE336/89, and must comply with the following
  standards :
  • IEC801-1: General surge protection requirements;
  • IEC801-2: Electrostatic discharges;
  • IEC801-3: Radiated Electro magnetic interference;
  • IEC801-4: Voltage transients – Fast transient bursts;
  • IEC801-5: Process equipment: surge immunity requirements.
• Tenderers shall make a specific statement in this regard. The word "Noted" or such other non-committal response will not be considered acceptable.

In addition, sensors must be fully resistant to RFI interference to a signal strength of 10 V/m over a frequency range of 1MHz to 1000 MHz, and a signal strength of over 50 V/m over Cellular Telephone signal bands:

- 850 MHz (TX: 824.2 - 848.8 MHz and RX: 869.2 - 893.8 MHz);
- 900 MHz (TX: 880.2 - 914.8 MHz and RX: 925.2 - 959.8 MHz);
- 1800 MHz (TX: 1710.2 - 1784.8 MHz and RX: 1805.2 - 1879.8 MHz);
- 1900 MHz (TX: 1850.2 - 1909.8 MHz and RX: 1930.2 - 1989.8 MHz);

Tenderers shall make a specific statement in this regard. The word "Noted" or such other non-committal response will not be considered acceptable.

over 50 V/m in the Wireless Local Area Network (WLAN) signal bands:

- 900 MHz (902 – 928 MHz);
- 2.4 GHz (2400 – 2483.5 MHz);
- 5.1 GHz (5150 – 5350 MHz);
- 5.4 GHz (5470 – 5725 MHz);
- 5.7 GHz (5725 – 5850 MHz);

Tenderers shall make a specific statement in this regard. The word "Noted" or such other non-committal response will not be considered acceptable.

over 50 V/m in the Bluetooth signal bands:

- 2.4 GHz (2402 – 2480 MHz);
- 2.4 GHz (2472 – 2497 MHz);

Tenderers shall make a specific statement in this regard. The word "Noted" or such other non-committal response will not be considered acceptable.
1.4 THREE-PHASE UNINTERRUPTIBLE POWER SUPPLY SYSTEM (STATIC, FREE-STANDING)

1.4.1 GENERAL

This section covers the standard specification for the supply, delivery, complete installation on site in full working order, testing, commissioning and maintenance of a Free Standing, Continuously Rated, Solid State Uninterruptible Power Supply (UPS) as specified. The UPS shall utilize true on-line, double conversion topology, whereby the output power supplied is derived directly from the UPS inverter without the need for an internal step-up output transformer. The UPS will be used to operate in conjunction with the existing building supplies and shall provide high quality power distribution for critical loads.

Full particulars, performance curves and illustrations of the equipment offered, shall be submitted with the Tender. Tenderers may quote for their standard equipment, complying as closely as possible with this Specification, but any deviations from the Specification shall be fully detailed.

The complete installation shall comply with the requirements of this specification. Should any discrepancies or contradictions occur between this part of the Specification and the Detailed Technical Specification then the latter shall take preference. Should any discrepancies between the written specification and the drawings become evident, the Contractor shall ascertain the position before tender closing date, otherwise the Engineer's decision will be binding.

This specification is of simplified form and includes abbreviated sentences. The omission of words or phrases shall be implied by inference. Unless clarified by the Contractor prior to submitting the tender, interpretation of clauses, words and phrases shall be as determined by the Consulting Engineer.

The Client reserves the right to accept any portion of any tender and does not bind itself to accept the lowest or any tender.

The Contractor is required to provide all material, equipment, labour and services and to perform all operations required for the installation to be complete and operative.

"Document" shall mean the complete set of Contract documents including all drawings, variation orders and Engineer's instructions issued in terms of the Contract.

The Engineer will inspect the installation from time to time during the progress of the work. Discrepancies will be pointed out to the Contractor and these shall be remedied at the Contractor's expense.

Under no circumstances shall the abovementioned inspections relieve the Contractor of his obligations in terms of these Documents. It is the responsibility of the Contractor to ensure that the materials supplied and the installation conforms fully to this specification.

The Contractor shall notify the Engineer timeously when the installation reaches important stages of completion (e.g., equipment installation, pressure testing, etc.) so that the Engineer's representative may schedule his site inspections in the best interests of all concerned. Work shall not be unduly closed up prior to inspection.

NO DEVIATION FROM THE SPECIFICATION will be tolerated or paid for without the written approval of the Engineer.

The installation shall comply in each instance with all relevant SABS codes of practice and standards.

Where no SABS guideline exists the BS, IEC and ANSI standards will be applicable.

At the end of each day, the Contractor shall be responsible for the cleanup, removal, and secure disposal of all debris.
1.4.1.1 STANDARDS

The installation shall be Erected and Tested in Accordance with the following Standards:

(a) OHSA The Occupational, Health and Safety Act, Act 85 of 1993.
(b) SANS The SANS Code for the Wiring of Premises - SANS 10142-1 as well as SANS 180-1974 as amended.

The product shall have CE marking in compliance with the following European directives:

(c) Low Voltage Directive – 2006/95/EC;
(d) EMC Directive – 2004/108/EC.

The local Municipal bylaws and regulations as well as the regulations of the Local Supply Authority.

(e) Code of Practice for Engineering Drawing (Metric Units).
(f) BS 308 : (Including Supplement No. 1) Engineering Drawing Practice.
(g) ISO Recommendation R370 : Conversion of Toleranced Dimensions.
(h) BS 3939 : Recommended Graphical Symbols.
(i) BS5486 Part 1:1977 : Factory Built Assemblies of Switchgear and Control Gear for Voltages up to and including 1000V AC and 1200V DC.
(j) BS5419:1977 : Air Break Switches, Air Break Disconnectors.
(k) IEC 148:1972 Air Break Switch Disconnectors and Fuse Combination Units for Voltages up to and including 100V AC and 1200V DC.
(m) IEC 144 : Degrees of Protection of Enclosures for Low Voltage Switchgear.
(n) IEC Technical : Draft guiding principles in the preparation of Sub-Committee circuit diagrams.
(o) BS4752-1:1977 : Circuit breakers of rated voltage up to and including 1000V AC and 1200V DC.
(p) BS 142:1966 : Electrical Protective Relays.
(q) BS89:1977 / IEC51 : Direct Acting Electrical Indicating Instruments.
(r) BS3693-1:1964 : Instruments of bold presentation and for rapid reading.
(s) BS3938:1973 : Current Transformers.
(t) BS3941:1975 : Voltage Transformers.
(u) BS3535:1962 : Safety Isolating Transformers for Domestic and Industrial Purposes.
(v) BS 588 : Cartridge Fuses for Voltages up to and including 1000V AC and 1500V DC.
(w) DIN 43620 : Low Voltage High Current Fuses 500V with Contact Blades - NH Fuse Cartridges.
(x) VDE 0660-4 : Regulations for Low Voltage Power Fuses (NH Fuses) with Rated Voltages up to 1000V AC and up to 3000V DC.
(y) IEC 269-1/-2 : Low Voltage Fuses.
(z) BS 158 : Marking and Arrangement of Switchgear Busbars, Main Connections and Small Wiring.
(aa) BS 159 : Busbars and Busbar Connections.
(bb) BS 1433 : Copper for Electrical Purposes.
(cc) BS 1706 : Electroplated Coatings of Cadmium and Zinc on Iron and Steel.
(dd) BS5472: 1977 Specification for Low Voltage Switchgear and Control Gear for Industrial use, Terminal Marking and Distinctive Number (General Rules).
(ee) BS4794-1:1973 : Control Switches, Switching Devices including Part 2:1977 Contactor Relays for Control and Auxiliary Circuits up to, and including 1000V AC and 1200V DC.
(ff) SANS 763:1977 Hot Dip (Galvanized) Zinc Coatings other than Continuously Coated Steel Sheet and Wire.
(hh) SANS 1091 National Colour Standards for Paint.
The Contractor shall issue all notices and pay all the required fees in respect of the installation to the authorities, and shall exempt the Client from all losses, claims, costs or expenditures which may arise as a result of the Contractor's negligence in not complying with the requirements of the regulations.

It shall be assumed that the Contractor is conversant with the abovementioned regulations. Should any requirements, bylaws or regulations, which contradict the requirements of this Document, apply or become applicable during erection of the installation, such requirements, bylaws or regulations shall overrule this Document and the Contractor shall immediately inform the Engineer of such a contradiction. Under no circumstances shall the Contractor carry out any variations to the installation in terms of such contradictions without obtaining written permission to do so from the Engineer.

The manufacturer shall further demonstrate conformity with the UPS harmonized standards and directives EN 62040-1-1 (Safety) and EN 62040-2 (EMC). The UPS shall be designed in accordance with the applicable sections of the current revision of the following standards. Where a conflict arises between these documents and statements made herein, the statements in this specification shall govern.

**Safety Standard:**

**Electromagnetic Compatibility Standard (EMC):**
- IEC 61000-3-3:2008 – Electromagnetic compatibility (EMC) – Part 3-3: Limits – Limitation of Voltage Changes, Voltage Fluctuations and Flicker in Public Low-Voltage Supply Systems, for Equipment with Rated Current ≤16 A per phase and Not Subject To Conditional Connection.

**Performance Standard:**

### 1.4.2 SCOPE

(a) The Contract shall include the complete manufacture, testing, supply, delivery, installation, commissioning, guarantee and maintenance during the guarantee period of the Uninterruptible Power Supply (UPS).

(b) The System shall Comprise of the following:

A Free Standing, Continuously Rated, Solid State Uninterruptible Power Supply (UPS), Each Capable of Delivering the Load Specified. Battery Cabinet(s) to neatly and safely house all required batteries for the UPS. All Power and Control Cabling between the Generating Set(s) and Control Board(s). Outlet Points, (as Installed), are in Accordance with the Contractors’ Requirements.

(c) The Following will be Provided by Others:
- Outgoing Supply from the Main Circuit Breakers.
- Plant Room Accommodation as shown on the Drawing.

1.4.3 MAKING GOOD

(a) The Contractor will be responsible for making good in all trades, damage or disturbance to the buildings, installation, tarred surfaces, concrete surfaces which he or his employees may have caused in the course of the installation of equipment. The Contractor will be responsible for keeping the site tidy and shall remove from the site all rubble and litter resulting from his work.

1.4.4 EQUIPMENT

(a) All equipment shall conform in respect of quality, manufacture, tests and performance, with the standards above.

(b) All equipment shall be of acceptable quality and suitable for the conditions on site. These conditions shall include weather conditions as well as conditions under which materials are installed, stored or used. Should the equipment not be suitable for use under temporary site conditions, then the Contractor shall at his own cost provide suitable protection until these unfavorable site conditions cease to exist.

(c) Locally manufactured equipment shall be used where possible and practical in preference to imported equipment. The Client in no way binds himself to assist the Contractor in obtaining import permits for imported equipment.

1.4.5 INSTALLATION

(a) All installation costs shall be incorporated in the tender.

(b) A system schematic diagram shall be prepared and mounted on the plant room behind clear Perspex.

1.4.6 PACKAGING, TRANSPORT, LOADING, STORAGE, SITE INFORMATION AND CONDITIONS

(a) The Contractor shall inform the Engineer of the Client, when the UPS is ready for installation.

(b) The Contractor is advised to visit the site and acquaint himself with all local conditions pertaining to the execution of the installation before tender closing date. No claims from the Contractor which may arise from insufficient knowledge of site access, type of site, labour conditions, establishment space, transport and loading/unloading facilities, power and water supply, etc., will be considered after submission of tenders.

(c) The set shall be suitably packed for transporting to the site from the factory. The cost of packing and transport shall be included in the tender price. The Contractor shall be responsible for the loading, transport to the site, off-loading, storage rigging into position and security of the equipment on site or elsewhere as required. The regulations of the South African Government regarding shipping, customs tariff and inspection shall be complied with.
1.4.7 ARRANGEMENTS WITH THE SUPPLY AUTHORITY

(a) The Contractor shall give all notices required by and pay all necessary fees, including any inspection fees, which may be required by the local Supply Authority unless otherwise specified.

(b) It shall be the responsibility of the Contractor to make the necessary arrangements at his own cost with the local Supply Authority and to supply the labour, equipment and means to inspect, test and commission the installation to the requirement of the Local and Supply Authorities.

(c) The Contractor shall supply and install all notices and warning signs that are required by the appropriate laws, regulations and/or the documents.

1.4.8 MATERIAL, EQUIPMENT AND WORKMANSHIP

(a) All material shall conform in respect of quality, manufacture, tests and performance, with the requirement of the South African Bureau of Standards or where no such standards exist, with the appropriate current specification of the British Standards Institution.

(b) All material shall be new and of acceptable quality and suitable for the conditions on site. These conditions shall include weather conditions as well as conditions under which materials are installed, stored or used. Should the materials not be suitable for use under temporary site conditions then the Sub-Contractor shall at his own cost provide suitable protection until these unfavorable site conditions cease to exist.

(c) The Contractor shall, where requested to do so, submit samples of equipment and materials to the Engineer for his approval prior to installation. Samples may be retained in the Engineer’s possession until the Contract is completed after which they will be returned.

(d) Locally manufactured equipment shall be used where possible and practical in preference to imported equipment. The Client in no way binds himself to assist the Sub-Contractor in obtaining import permits for imported equipment.

(e) The works shall be so installed as to provide ease of inspection, cleaning and maintenance.

(f) All artisans employed on site shall be competent in terms of the Regulations and Acts. All installations shall be carried out by qualified artisans or under the direct supervision of qualified artisans. Installations (or part thereof) carried out by unskilled persons will be rejected.

(g) The Contract shall be executed to an acceptable standard and to the satisfaction of the Engineer. Should any workmanship, equipment or material not be to the satisfaction of the Engineer, it shall be rectified at the cost of the Contractor and all rejected materials shall be removed from site.

(h) If, in the opinion of the Engineer, any member of the Contractor’s staff is not competent to carry out the work to the required standard, then that person shall be removed from the project if so instructed by the Engineer.

1.4.9 PROGRAMME AND PROGRESS

(a) The programme for carrying out the works shall be submitted in detailed form covering all significant operations and shall be in the form of a Gantt Chart (preferably in Microsoft Project Format). In addition, should the information be required in a particular format to suit project management requirements then such information shall be provided as part of this Contract.

(b) The Contractor shall liaise with all necessary parties (other Contractors, Sub-Contractors, Consultants, Equipment Suppliers, etc.) to ensure that the programme is as accurate and as realistic as possible.
(c) The Contractor shall submit the programme as soon as possible after award of the Contract but at the latest fourteen (14) days after award of the Contract.

(d) The programme shall list each scheduled item of equipment in the Contract and shall indicate periods for:
   - Preparation, Approval and Finalization of Manufacturing Drawings;
   - Ordering;
   - Manufacturing;
   - Inspection and Testing during Manufacture;
   - Delivery;
   - Installation;
   - Testing;
   - Commissioning.

(e) The Contractor shall build into the programme, a period of two weeks, for approval of drawings by the Engineer.

(f) The Contractor shall allocate to a senior member of his staff the duties of studying and evaluating the works in relation to the approved programme, of devising methods to overcome or prevent delays and of co-operating with the Engineer and other Contractors working on site. He shall report to the Engineer and draw his attention timeously to anything, which may cause a delay in the execution of the works.

(g) The programme shall be updated as and when necessary to take account of changed circumstances.

1.4.10 CO-OPERATION WITH OTHER TRADES

(a) The Contractor shall ascertain the extent of the work of other trades on site, which may affect, or be affected by the Contractor's installation.

(b) The Contractor shall give all necessary assistance reasonably required to other trades to ensure that the work of such trades can be installed satisfactorily and without delay.

(c) The Contractor shall liaise with other trades working in close proximity to the work, covered by this specification, and shall assist in working out equipment and material positions to ensure that all trades can complete their work satisfactorily.

1.4.11 BUILDER'S WORK

(a) The Contractor shall, within seven (7) days, or any shorter period, which may be necessitated by the construction programme, submit two (2) copies of all drawings showing all builders' work required for the project.

(b) The drawings shall provide the builder with all the dimensions, details, etc., for the work to be carried out correctly. The Engineer will scrutinize the drawings and request changes and adjustments as required. After such changes are satisfactorily made the Engineer will fix his stamp of approval to the drawings.

(c) The Contractor shall provide all the necessary copies of the drawings to the Engineer for issue to all parties.

(d) It is the responsibility of the Contractor to check the builder's work as it is completed to ensure that the work has been correctly carried out in accordance with the drawings. The Contractor shall point out any problem areas as soon as possible to the builder so that they can be rectified. No claims will be considered for delays or other additional costs which arise out of the Contractor's failure to check the builder's work in good time.

(e) The builder's work drawings shall be fully dimensioned and shall include the following:
   - Details of all Plant Bases Required;
   - Details of all Openings in Walls and Concrete Work Required;
   - Details of Ventilation Required;
   - Details and Positions of all Equipment to be Built into Walls;
Any Other Work Required.

(f) All areas where the installation pierces waterproofing shall be carefully finished and sealed by the Contractor and Builder to the approval of the Engineer and Architect. All necessary sleeves, caulking and flashing as required to make the installation waterproof shall be provided as part of this Contract.

1.4.12 SUPERVISION AND SITE ORGANISATION

(a) For the full duration of this Contract the Contractor shall employ at least one good and competent Supervisor, skilled in all aspects of the trades and skills required by the Contract. This supervisor shall be on site whenever work, associated with this Contract, is being carried out and shall at all times be available to attend to queries by the Principal Contractor or Engineer.

(b) The supervisor shall be the Contractor's authorized representative for the project and shall be available to attend progress meetings when called upon to do so by the Principal Contractor, Engineer or Architect whether or not these take place prior to work actually starting on site.

(c) The supervisor shall be empowered to make all decisions necessary for the execution of the Contract.

(d) The supervisor shall not be transferred from his position without approval of the Engineer.

(e) The Contractor shall at all times have on site copies of all relevant drawings as well as a copy of the specification. The Contractor shall institute the necessary procedures to ensure that the drawings on site are the latest drawings and that all superseded drawings are removed from site.

1.4.13 DRAWINGS

(a) The Engineer's drawings for the Contract shall be those issued at the times of tender together with any others issued to cover the variations to the Contract.

(b) As part of this Contract the Contractor shall provide the following Drawings:

   Manufacturing and Installation Drawings:
   The manufacturing and installation drawings ("shop drawings") shall provide all details of the components necessary for the manufacture and installation of the system in accordance with the specification.

   Wiring Diagrams:
   The wiring diagrams shall provide details of all the wiring associated with the installation.
   The same drawing symbols and system shall be used, as used on the Engineer's Drawings.

   Builder's Work Drawings:
   All necessary builders' work drawings, as described elsewhere in this specification, shall be provided as part of this Contract.

   AS BUILT Drawings:
   On completion of the installation, but before the plant is handed over; the Contractor shall provide a complete set of drawings showing the completed installation including wiring.

(c) In addition to the drawings listed above, the Contractor shall provide all drawings necessary for the execution of the Contract and shall submit such general and detailed drawings of the components and apparatus, as the Engineer may require approving construction of the system.

(d) Details and drawings of all major items of equipment, made by the Contractor or his suppliers, shall be submitted for approval without specific request from the Engineer.

(e) All required drawings shall be submitted to an agreed programme to suit the construction of the system.
All drawings shall be clearly numbered or marked with the equipment item numbers, area references etc.

1.4.13.1 APPROVAL OF DRAWINGS

(a) The Contractor shall submit, for approval, copies of all abovementioned drawings prior to starting work or issue to other parties. Any work started (off site or on site) prior to receiving the Engineer's approval of drawings shall be at the Sub-Contractor's own risk.

(b) The Engineer may require from the Contractor further detailed drawings and/or calculations, which clarify features not adequately shown on the layout drawings. The request for additional details shall not be construed as extending the scope of this Contract or altering the programme.

(c) The Contractor shall submit three copies of each drawing to the Engineer for approval.

(d) The Engineer will return to the Contractor, within two weeks of their receipt by him one copy of each drawing marked 'APPROVED IN PRINCIPLE' or marked with any changes, which are necessary. The Contractor shall modify the details and drawings as required by the Engineer. The nature and date of each modification and a distinguishing symbol shall be added and the drawings shall be submitted again for approval.

(e) Alterations to drawings, by the Engineer, are not intended to change the scope of the work unless explicitly stated as doing so. Should any alterations, in the opinion of the Contractor, change the scope of work the Contractor shall notify the Engineer immediately of receipt of the altered drawings before any further drawing work or fabrication is carried out. Claims for a change of scope, made after performance of the work constituting the claimed change of scope of work will not be considered.

(f) The approval in principle of drawings by the Engineer shall not relieve the Contractor of any responsibility in terms of the Contract. The Engineer will check the drawings for design only and approval of the drawings, schedules and catalogues shall not be construed as a complete check.

(g) The Contractor shall be responsible for any discrepancies, errors or omissions in the drawings and other particulars supplied by him whether such drawings or particulars have been approved by the Engineer or not, provided that such discrepancies, errors or omissions are not due to inaccurate information or particulars furnished in writing to the Contractor.

(h) The Contractor shall provide, at his own expense, all copies of drawings required by him in the execution of the work and shall also, at his own expense, supply to the Engineer such drawings and copies thereof as are provided for in the specification.

(i) On completion of the installation, but before final handover, the Contractor shall provide three high quality paper prints of each of the Contract drawings showing the system as fixed. These Drawings will be folded and included in the AS BUILT Documentation. The Drawings shall include, but not be limited to:

- Complete 1:50 Scale Layouts of Plant Rooms;
- Complete 1:100 Scale Drawings of the Whole Installation;
- Detailed Drawings of All Items of Plant;
- Electrical Layouts and Wiring Diagrams;
- Details of Any Other Items Requested by the Engineer.

(j) The drawings shall be sufficient in detail to enable the Client's staff to maintain, dismantle, reassemble and adjust any part of the works.
1.4.14 CABLING

1.4.14.1 GENERAL

Supply, install, connect, and terminate all cabling necessary to complete the installation, including all power and UPS distribution, data, control, fibre-optic (where applicable), communications cabling and device cabling.

1.4.14.1.1 CABLE CONNECTION

(a) The Contractor will be responsible for all electrical cable connections associated with the complete UPS installation.

1.4.15 INFORM

(a) The Contractor shall inform the Engineer when the set is ready for installation.

1.4.16 OPERATION

(a) The set is required to supply the lighting and power requirements as specified by the Engineer in the case of a mains power failure.
(b) The set shall be fully automatic i.e. it shall start when any one phase of the main supply fails or get switched and shall shut down when the normal supply is re-established. In addition it shall be possible to manually start and stop the set by means of pushbuttons on the switchboard.
(c) The automatic control shall make provision for three consecutive starting attempts. Thereafter the set shall be switched off, and the start failure relay on the switchboard shall give a visible and audible indication of the fault.
(d) To prevent damage to the system a safe and fail proof system of suitably interlocked contactors shall be supplied and fitted to the changeover switchboard.

1.4.16.1 IMPORTANT NOTE

(a) The Contractor shall submit, together with his offer, the design of the control system to comply with the requirements for automatic starting, stopping, interlocking and isolation as specified.

1.4.16.2 MARKINGS

(a) All labels, markings or instructions on the switchgear shall be in English.

1.4.16.3 EARTHING

(a) A solid copper earth bar of at least 40mm x 10mm shall be fitted in the switchboards to which all non-current carrying metal parts of the switchboard shall be bonded.
(b) The neutral point of the alternator shall be solidly connected this bar by means of a removable link labelled “EARTH”. Suitable terminals shall be provided on the earth bar for connection of up to three earth conductors, which will be supplied and installed by others.
(c) The outer casing of the alternator, the engine and all parts of the base frame shall also be earthed to this bar.
(d) The size of the earth conductors shall comply with the Code of Practice for the Wiring of Premises, SANS 10142 as amended.
1.4.17 INSTALLATION

(a) Except for the supply of the incoming mains cable and outgoing feeder cables, the Contractor shall include for the complete installation and wiring of the plant in running orders, including the connection of the incoming cable and outgoing feeder cables.

(b) The connecting of the cable and control cabling to the generator and the control terminals in the LV board remains the responsibility of the Contractor.

1.4.18 SYSTEM DESCRIPTION

1.4.18.1 GENERAL

The UPS system shall consist of a single UPS unit or the appropriate number of UPS units connected in parallel for operation in capacity or N+n redundancy mode. For a parallel installation all UPS units must operate simultaneously and equally share the load, without the need for either a centralized static bypass switch or system control cabinet.

1.4.18.2 PARALLEL INSTALLATION

1.4.18.2.1 CAPACITY (NON-REDUNDANT) SYSTEMS

All the UPS units connected in parallel are required to supply the full rated load. If a UPS unit power or control module should malfunction, the load is to be transferred automatically to the bypass line via each of the UPS units with their static bypass switches being triggered simultaneously. The battery set should consist of at least two strings so that in the event of a battery malfunction the affected string is automatically isolated from the system thereby ensuring battery autonomy is retained, albeit of a shorter duration.

1.4.18.2.2 REDUNDANT OPERATION

The UPS system will operate in an N+n configuration where N is the number of UPS units connected in parallel to support the load and n is the number of UPS units connected in parallel to provide the coefficient of redundancy. The parallel UPS units shall be capable of operation from a common DC bus or with a separate DC supply for each UPS unit. In either case the batteries should be configured so that the failure of one battery string (common DC bus) or the failure of one battery set (separate DC supply for each UPS) provides battery redundancy whereby the specified autonomy at full load is maintained. The malfunction of one of the UPS unit’s power or control modules shall cause that particular UPS unit to be automatically isolated from the system and the remaining UPS units shall continue to support the load. Replacement or repair of a UPS unit shall be achieved without disturbance to the connected load.

1.4.18.3 MODES OF OPERATION

The UPS shall be designed to operate as a true on-line, double conversion, Voltage and Frequency Independent (VFI) system where the UPS output is independent of supply (utility/generator) voltage variations, and frequency variations are controlled within EN 61000-2-2 limits.

The following modes of operation shall apply:

Normal – The critical AC load is continuously supplied directly by the UPS inverter. The UPS input free running rectifier derives power from the utility or generator AC source and supplies DC power to the inverter. A separate but integral battery charger shall maintain a ripple free float-charge voltage to the battery.
Battery – Upon failure of the input AC power supply the critical AC load is supplied by the inverter, which obtains power from the battery. There shall be no interruption in power to the critical load upon failure or restoration of the utility or generator AC source.

Recharge – Upon restoration of utility or generator AC power after a power outage, the input rectifier shall automatically restart and resume supplying power to the inverter and the battery charger shall recommence recharging the battery. The UPS input rectifier shall provide a soft start on the return of the utility or generator AC power. For parallel configurations, each UPS unit shall switch on sequentially with a switch on delay of between approximately 5 to 10 seconds.

Automatic Restart – Upon restoration of utility or generator AC power, after an AC power outage and after a complete battery discharge, the UPS unit(s) shall automatically restart and resume supplying power to the connected load via the inverter.

Static Bypass – The static bypass shall provide an alternate path for power to the connected AC load and shall be capable of operating in the following manner:

- **Single UPS Installation**:
  - Automatic – in the event of a UPS failure or should the inverter overload capacity be exceeded the UPS unit shall perform an automatic transfer of the connected AC load from the inverter to the bypass source.
  - Eco-Mode – The UPS unit shall be able to operate in Eco-Mode when the power quality parameters of the by-pass source are within the permissible tolerances. The UPS system shall automatically transfer the load to normal mode if the by-pass source goes out of permissible tolerances. Transfer in both directions shall be less than 5ms.
  - Manual – Should the UPS unit need to be taken out of service for limited maintenance or repair, manual activation of the bypass shall cause an immediate transfer of the connected AC load from the inverter to the bypass source. Full electrical isolation of the UPS system shall therefore be obtained, without disruption to the critical load, by operation of a separate wrap-around maintenance bypass.

- **Parallel UPS Installation**:
  - Automatic – In the event of a UPS failure the faulty UPS unit shall automatically disconnect itself from the critical bus without affecting the critical load. If the remaining UPS unit(s) are unable to support the load, e.g. an overload condition, all the UPS units (including the faulty module) shall perform an automatic transfer of the connected AC load to the bypass source via each of their internal static bypass switches.
  - Manual – Should all the UPS units need to be taken out of service for limited maintenance or repair, manual activation of the static bypass switch on one of the UPS units shall cause an immediate transfer of the connected AC load to the bypass source via each of the UPS units’ internal static bypass switch. Full electrical isolation of the UPS system shall therefore be obtained, without disruption to the critical load, by operation of the wrap-around maintenance bypass switch located in the UPS parallel switch panel.

1.4.19 PERFORMANCE REQUIREMENTS

The UPS shall be a true on-line double conversion, Voltage and Frequency Independent (VFI) technology in accordance with Standards SANS 62040-3:1999. The UPS shall be provided with the facility for paralleling for capacity or redundancy without limitation on the number of UPS units connected in parallel.

1.4.19.1 AC INPUT TO UPS

Voltage Configuration:

- 400/230 VAC Nominal, 3Ø, 4-Wire-Plus-Ground;
- 400/240 VAC Nominal, 3Ø, 4-Wire-Plus-Ground;
- 415/240 VAC Nominal, 3Ø, 4-Wire-Plus-Ground;
• 380/220 VAC Nominal, 3Ø, 4-Wire-Plus-Ground.

Input Frequency: 45 to 65 Hz, without switching to battery supply;
Input Current Distortion: Sinewave <9% THDi maximum at 100% rated load, 400/240 VAC;
Input Power Factor:
  • Equal to or greater than 0.98 at 100% Rated Load;
  • Equal to or greater than 0.94 at 50% Rated Load (Lagging).

Inrush Current: Limited by Softstart;

The Input Voltage Window shall be as shown in the table below, based on a Nominal Input Voltage of 240/400V and according to the Output Load of the UPS. Within the Input Voltage Range shown below the UPS shall not draw power from the Batteries to Support the Load.

<table>
<thead>
<tr>
<th>Load (% of UPS Rating)</th>
<th>Input Voltage (Lower Limit)</th>
<th>Input Voltage (Upper Limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>-20%</td>
<td>+15%</td>
</tr>
<tr>
<td>90-99</td>
<td>-23%</td>
<td>+15%</td>
</tr>
<tr>
<td>80-89</td>
<td>-26%</td>
<td>+15%</td>
</tr>
<tr>
<td>70-79</td>
<td>-30%</td>
<td>+15%</td>
</tr>
<tr>
<td>60-69</td>
<td>-35%</td>
<td>+15%</td>
</tr>
<tr>
<td>&lt;60</td>
<td>-40%</td>
<td>+15%</td>
</tr>
</tbody>
</table>

1.4.19.2 AC OUTPUT

(a) Output Rating:
  • Single UPS Installation – Continuously Rated at XXX kVA /0.8 pf;
  • Parallel UPS Installation – N+1 Parallel Redundant, Continuously Rated at XXX kVA/0.8 pf.

(b) Voltage Configuration:
  • 400/230 VAC Nominal, 3Ø, 4-Wire-Plus-Ground;
  • 400/240 VAC Nominal, 3Ø, 4-Wire-Plus-Ground;
  • 415/240 VAC Nominal, 3Ø, 4-Wire-Plus-Ground;
  • 380/220 VAC Nominal, 3Ø, 4-Wire-Plus-Ground.

(c) Voltage Tolerance:
  • Static ± 1% (0-100-0 Load Steps);
  • Dynamic ± 4% (0-100-0 Load Steps).

(d) Frequency Regulation: 50 or 60 Hz, ± 0.1%;

(e) Frequency Slew Rate: 2.0 Hertz per second maximum;

(f) Bypass Frequency Synch Range: ± 4% (Programmable);

(g) Voltage Distortion:
  • ± 1 % Total Harmonic Distortion (THD) maximum – 100% Linear Load.
  • ± 4% Total Harmonic Distortion (THD) maximum -100% Non-Linear Load with Crest Factor Ratio of 3:1.

(h) Load Power Factor Range:
  • 0.95 Leading to 0.8 Lagging without Derating;

(i) Load Peak (Crest) Factor: 3:1 minimum;

(j) Load Imbalance: 100% (All 3 Inverter Phases shall be Regulated Independently)

(k) Overload Capability:
  • 125% Load for a minimum of 10 minutes;
  • 150% Load for a minimum of 60 seconds.

(l) If the Overload Limits or Times are Exceeded the UPS will Transfer the Load to Bypass (if available) via the Static Transfer Switch.

(m) Transient Recovery Time: Within 1% of Steady State Output Voltage within 20 milliseconds;
1.4.19.3 UPS EFFICIENCY

The overall efficiency (AC-DC-AC, on-line mode) shall not be less than the figures shown in the table below:

<table>
<thead>
<tr>
<th>UPS Unit Rating</th>
<th>Load 100%</th>
<th>Load 75%</th>
<th>Load 50%</th>
<th>Load 25%</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=60kVA</td>
<td>95</td>
<td>95</td>
<td>94</td>
<td>91</td>
</tr>
<tr>
<td>&gt;60kVA</td>
<td>96</td>
<td>96</td>
<td>95</td>
<td>92</td>
</tr>
</tbody>
</table>

Measurement with Linear Load (Cos θ = 0.8 ind.)

1.4.19.4 BATTERIES

(a) The battery system shall be sized to support a connected load of XX (0.8 pf) for a minimum of XX minutes at an ambient temperature of 25 °C.

(b) The battery system shall consist of gas recombination, valve regulated, lead acid cells, compliant with BS 6290-4:1997 and BS EN6089-2. Flame retardant batteries shall be provided, which renders the UPS suitable for installation inside a computer room.

(c) The UPS battery charging circuit shall comprise of a separate battery charger and not depend on a charge voltage being derived from the UPS input rectifier. Consequently the battery charging voltage shall have zero AC (ripple) content.

(d) For single UPS systems the battery system shall consist of a minimum of 2 parallel strings of multiple cells. Each individual parallel string shall have its own dedicated means of electrical protection.

For multiple UPS units connected in parallel the battery system shall be either;

- A common battery feeding all the UPS units. In this case the battery system shall consist of a minimum of two parallel strings of multiple cells. Each individual string shall have its own dedicated means of electrical circuit protection.
- A separate battery system for each individual UPS unit. In this case each separate battery system may consist of one protected string of multiple cells. If two or more parallel strings are used then each individual string shall have its own dedicated means of electrical circuit protection.

For all the above battery system arrangements the batteries shall be configured so that in the event of a battery malfunction the affected string is automatically isolated from the system thereby ensuring battery autonomy is retained (see System Description 1.3.2).

(e) The batteries shall be housed in cabinet/s comprising a floor-standing steel enclosure with dimensions and paint finish to match the UPS system cabinet/s to form a continuous suite when standing immediately adjacent to the UPS system cabinet/s. The battery cabinet/s shall have full width opening doors to permit ease of access for the purposes of maintenance and/or repair of the batteries.

Alternatively, the batteries shall be housed on open or cladded racks of a steel construction, having an epoxy powder-coated finish, with adjustable feet for leveling and adequately designed to support the weight of the batteries and permit ease of access for the purposes of maintenance and/or repair of the batteries. If the battery system is located on open stands then all individual battery cell terminals shall be fully shrouded to prevent inadvertent contact.

(f) A fully discharged battery system shall be capable of being recharged to 80% of the UPS output capacity within a maximum period of 10 times the normal total discharge time period, and to 90% of the UPS output capacity within a maximum period of 4 hours.

(g) The UPS DC bus voltage shall be variable whereby the number of battery blocks can be adjusted between 40 to 50 (12 VDC blocks) or 80 to 100 (6 VDC blocks) to enable the battery system to be optimized for size and cost.
The Lead Acid Battery installation shall comply to the following Standards:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS 6290-4:1997</td>
<td>Lead-acid stationary cells and batteries. Specification for classifying</td>
</tr>
<tr>
<td></td>
<td>valve regulated types.</td>
</tr>
<tr>
<td>BS EN 60896-1:1992, IEC</td>
<td>Stationary lead-acid batteries. General requirements and methods of test.</td>
</tr>
<tr>
<td></td>
<td>Vented type.</td>
</tr>
<tr>
<td></td>
<td>Valve regulated type.</td>
</tr>
<tr>
<td>BS EN 50272-2:2001</td>
<td>Safety requirements for secondary batteries and battery installations.</td>
</tr>
<tr>
<td></td>
<td>Stationary batteries.</td>
</tr>
<tr>
<td>ANSI/IEEE 450-2002</td>
<td>IEEE recommended practice for maintenance, testing and replacement of</td>
</tr>
<tr>
<td></td>
<td>vented lead-acid batteries for stationary applications.</td>
</tr>
<tr>
<td>ANSI/IEEE 1184-1994</td>
<td>IEEE recommended guide for selection and sizing batteries for</td>
</tr>
<tr>
<td></td>
<td>Uninterruptible Power Supplies (UPS).</td>
</tr>
<tr>
<td>ANSI/IEEE 1188-1996</td>
<td>IEEE recommended practice for maintenance, testing and replacement of</td>
</tr>
<tr>
<td></td>
<td>valve-regulated lead-acid (VRLA) batteries for stationary applications.</td>
</tr>
</tbody>
</table>

1.4.20 ENVIRONMENTAL CONDITIONS

(a) The UPS system shall be designed to operate continuously at full load without degradation of its reliability, operating characteristics or service life in the following environmental conditions:
   - UPS Ambient Temperature Range: 0°C to 40°C;
   - Battery Ambient Temperature Range: 20°C to 25°C;
   - Humidity: 5 to 95% RH Non-Condensing.

(b) The UPS system shall be designed for operation in altitudes up to 1000 metres, without the need for derating or reduction of the above environmental operating temperatures.

(c) The audible noise generated by the UPS system during normal operation shall not exceed 73 dBA measured at 1 metre from the surface of the UPS.

(d) The UPS system shall be able to withstand a minimum 15kV electrostatic discharge without affecting the critical load.

(e) The maximum floor load of the UPS system cabinet (excluding batteries) shall not exceed a UDL of 8.0 kN/m².

(f) To permit access through a standard single doorway opening, either the width or the depth of the UPS and battery cabinets shall not exceed 750mm.

(g) The UPS system cabinet shall comprise of a floor standing steel enclosure to house the power system, control systems, battery connections and all associated switchgear necessary for the correct operation of the UPS in accordance with the requirement of the specifications. All switchgear and interconnections must be adequately protected to enable an isolated section to be safely maintained or repaired whilst the remaining system supports the load.

(h) The UPS system shall be designed to limit the injection of current harmonics in to the incoming utility supply and as such the maximum total input current harmonic distortion should not exceed 10% THD$i$ when the UPS system is operating at the UPS manufacturer’s specified rating.

1.4.21 OTHER EQUIPMENT

The following additional equipment shall be supplied and installed by the Contractor:

A Wall Chart containing bilingual step-by-step checking procedures in the event that the UPS does not start.
1.4.22 WARNING NOTICES

Notices, in English shall be installed in the plant-rooms.

The contents of these notices are summarized below:

Unauthorized entry prohibited.
Unauthorized handing of equipment prohibited.
Procedure in case of electric shock.
Procedure in case of fire.

The successful tender shall consult the Act and get approval of the wording from the Client’s representative, prior to ordering the notices.

Lettering shall be black on a yellow background.

Notices (a) shall be installed outside next to the entrance of the plant-room and
(b-d) inside the plant-room.

In the plant-room, a clearly legible and indelible warning notice shall be mounted in a conspicuous position.

The motive shall be made of a non-corrodible and non-deteriorating material, preferable plastic, and shall be read as follows:

DANGER : This should always be considered ‘LIVE’. Turn selector switch on control board to “OFF” before working on the plant.

GEVAAR : Hierdie toerusting moet altyd as ‘LEWENDIG’ beskou word. Draai keuseskakelaar op beheerpaneel na "AF" voordat aan die toerusting gewerk word.

1.4.23 INFORMATION REQUIRED

(a) Tenderers shall furnish detailed descriptions and illustrations of the equipment offered and shall complete the questionnaire following this specification. This includes drawings of the switchboard layouts and control diagrams.

(b) Failure to submit any of the information asked for may disqualify the tender.

1.4.24 REMOTE MONITORING

(a) Voltage free, N/O alarm contacts from all the major protection devices shall be wired to a separate terminal box in the control board. All wiring and terminals shall be clearly identified in accordance with the relevant wiring diagrams.

(b) All outgoing wiring from this terminal box will be done as part of this contract.

(c) On this installation a mimic panel accommodating all the major protection devices shall not be provided in a remote position. Reset must be done at the plant room.

1.4.25 TOOLS AND EQUIPMENT

(a) Unless otherwise specified, the Contractor shall provide all tools, materials, scaffolding, power, water, etc., necessary for the proper and efficient execution of the work covered by this specification.

(b) No extra payment will be made for plant, equipment, materials required by the Contractor to complete the work.
(c) The Contractor shall provide all rigging, cranes, lifting, equipment, etc., necessary to execute the works.

1.4.26 STORAGE OF EQUIPMENT AND MATERIALS

(a) The Contractor shall ensure that all stored materials and equipment are safely stacked and that stacking does not damage them.

(b) The Contractor shall ensure that stored materials and equipment do not overload the structure or floor construction.

(c) The storage of combustible materials on site shall be kept to a minimum. The Contractor shall be responsible for ensuring that such combustible materials are safely stored. Suitable fire fighting equipment shall be provided by the Contractor, who shall further ensure that staff capable of using the equipment is at hand.

1.4.27 LOCATION OF EQUIPMENT

(a) The Contractor shall check on doorways, passages, openings, lifts, etc. provided and shall ensure that all equipment offered can be moved through them to its final position. If necessary, equipment shall be ordered in a partially dismantled condition so that it is suitable for moving through the restricted openings or areas of restricted height or areas of restricted load.

1.4.28 PRODUCT

1.4.28.1 FABRICATION

(a) Construction:
   - All materials and components making up the UPS shall be new, of current manufacture, and shall not have been in prior service except as required during factory testing. The UPS shall be constructed of replaceable sub-assemblies.

(b) Wiring:
   - Wiring practices, materials, and coding shall be in accordance with the requirements of the EN 50091 and other applicable British and European codes and standards.

(c) UPS Cabinet:
   - The UPS system cabinet shall offer a minimum degree of protection to the EN 60529 standard, IP20 code. The UPS cabinet shall be cleaned, primed and painted in RAL 9002. Either the width or the depth of the UPS cabinet should not exceed 750mm, to permit access through a standard doorway.

(d) Battery Cabinet:
   - The battery cabinet shall offer a minimum degree of protection to the EN 60529 standard, IP20 code. The battery cabinet shall be cleaned, primed and painted to RAL 9002 and should match the UPS cabinet(s) in appearance and height. Either the width or the depth of the battery cabinet should not exceed 750mm to permit access through a standard doorway.

(e) Battery Racks:
   - The battery racks shall be of a steel construction, having an epoxy powder-coated finish, with adjustable feet for levelling. Open racks shall not exceed 2 meters in height to the top tier and should not be more than 2 rows deep if it is not possible to gain rear access, e.g. the rack is placed against a wall. Cladded racks shall offer a minimum degree of protection to the EN 60529 standard, IP20 code and the panels shall be cleaned, primed and painted to RAL 9002.
Cooling:
- The UPS shall be forced-air cooled by internally mounted fans.

1.4.28.2 COMPONENTS

(a) Input Converter:
- General:
  Incoming AC power shall be converted to a regulated DC output by the input converter for supplying DC power to the inverter. The input converter shall provide input power factor and input current harmonic distortion correction. 12 Pulse Rectifier and/or Filter Devices will not be accepted if they have a detrimental effect on the overall UPS efficiency.
- AC Input Current Limit:
  The input converter shall be provided with AC input over current protection.
- Input Protection:
  The UPS shall have built-in protection against undervoltage, overcurrent, and overvoltage conditions, including low-energy surges introduced on the primary AC source and the bypass source. The UPS cabinet shall not contain an input circuit breaker. The electrical contractor shall supply an input circuit breaker/fuse sized to supply the rated load and to recharge the battery at the same time.
- Battery Recharge:
  To prolong battery life, the UPS shall have the facility for automatically adjusting the battery charging voltage according to the environmental temperature of the batteries. The battery charger shall be ripple-free avoiding premature battery ageing.

(b) Inverter:
- General:
  The inverter shall convert DC power from the input converter output, or the battery, into precise regulated sinusoidal wave AC power for supporting the critical AC load.
- Overload:
  The inverter shall be capable of supplying current and voltage for overloads exceeding 100% and up to 200% of full load current. A visual indicator and audible alarm shall indicate overload operation. The load shall be immediately transferred to bypass when the load current exceeds this level of overload. In the event the bypass supply is unavailable (e.g. mains failure), the inverter shall have electronic current-limiting protection to prevent damage to internal components. The inverter shall be self-protecting against any magnitude of connected output overload and the inverter control logic shall sense and disconnect the inverter from the critical AC load within 200 ms.
  The inverter shall be capable of supplying the following overload currents:
  - 125% For 10 minutes
  - 200% For 10 seconds
- Output Frequency:
  The output frequency of the inverter shall be controlled by an oscillator. The oscillator shall hold the inverter output frequency to ± 0.1% for steady state and transient conditions. The inverter shall synchronise with the bypass supply assuming the bypass supply stays within the selected range. If the bypass source fails to remain within the selected range, the inverter shall revert to the internal oscillator.
- Battery over Deep Discharge Protection:
  To prevent battery damage from deep discharging, the UPS control logic shall monitor the discharge voltage and shut the UPS down at a pre-set minimum DC voltage. This level is dependent on the rate of discharge and battery autonomy and shall be adjusted at the time of commissioning the UPS.
equipment. Under any circumstances it should not be set to less than 1.67V per cell.

(c) Display and Controls:

• General:
The UPS front panel shall consist of multiple status LEDs, switches, and an alphanumeric LCD display for additional alarm/configuration information. During normal operation (on-line), all mimic display LEDs shall be green in colour and indicate the following:

<table>
<thead>
<tr>
<th>Line 1</th>
<th>(AC Input rectifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 2</td>
<td>(AC Input by-pass)</td>
</tr>
<tr>
<td>Battery</td>
<td>(Load supplied from the battery)</td>
</tr>
<tr>
<td>On Inverter</td>
<td>(Load supplied from the inverter)</td>
</tr>
<tr>
<td>On Bypass</td>
<td>(Load supplied from the bypass)</td>
</tr>
</tbody>
</table>

A UPS fault shall be identified via additional indicators and audible alarms to notify the user that a UPS fault condition has occurred. During mains failure the colour of the LED’s shall be as follows:

<table>
<thead>
<tr>
<th>Line 1</th>
<th>(AC Input rectifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 2</td>
<td>(AC Input by-pass)</td>
</tr>
<tr>
<td>Battery</td>
<td>(Load supplied from the battery)</td>
</tr>
<tr>
<td>On Inverter</td>
<td>(Load supplied from the inverter)</td>
</tr>
<tr>
<td>On Bypass</td>
<td>(Load supplied from the bypass)</td>
</tr>
</tbody>
</table>

If there is a fault condition, the UPS shall attempt to maintain conditioned power to the load or at minimum transfer to bypass. In addition to a visual fault signal (alarm), the UPS shall also record fault occurrences in a rolling event log. The event log shall record up to 64 occurrences, with the oldest events discarded first, etc. The user shall have access to the event log through the LCD display. Every alarm and/or event recorded in the event log will contain a time and date stamp.

• Audible Alarms:
The volume of all audible alarms shall be at least 65 dBA at a distance of one meter. An audible alarm shall be used in conjunction with the LED/LCD display to indicate a change in UPS status. The audible alarms shall warn loss of mains or generator supply, low battery (whilst on battery), and all other alarm conditions. For all audible alarm conditions, the display shall identify the cause of error/alarm. All alarm tones shall be a continual tone until the condition rectifies itself or the alarm is silenced. Once silenced, the audible alarm shall not sound until a new alarm condition is present, but the LED indication shall continue to identify the alarm condition.

• Alarm Silence Button:
The display panel shall include an audible alarm ‘Reset’ switch. If the alarm mute (Reset) switch is pressed for one second, all current audible alarms shall be disabled. If a new alarm occurs, or a cancelled alarm condition disappears and then re-appears, the audible alarm is re-enabled.

• LCD Display:
The LCD display shall be used to provide the following information to the user and UPS service engineer:

<table>
<thead>
<tr>
<th>Phase Voltages</th>
<th>Input To Converter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input To By-Pass</td>
</tr>
<tr>
<td></td>
<td>UPS Output</td>
</tr>
<tr>
<td>Battery</td>
<td>DC Voltage (Voltage To/From Battery)</td>
</tr>
<tr>
<td>Current</td>
<td>UPS Output (Line Current)</td>
</tr>
<tr>
<td></td>
<td>Battery Charging/Discharging</td>
</tr>
</tbody>
</table>
### Frequency Table

<table>
<thead>
<tr>
<th></th>
<th>UPS Input</th>
<th>UPS Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomy</td>
<td>Remaining Back-Up Time (Minutes)</td>
<td>Battery Capacity (%)</td>
</tr>
<tr>
<td>Others</td>
<td>UPS Output Active Power (kW)</td>
<td>UPS Output Reactive Power (kVA)</td>
</tr>
<tr>
<td></td>
<td>UPS Output Reactive Power (kVA)</td>
<td>UPS Output Apparent Power (kVA)</td>
</tr>
<tr>
<td></td>
<td>UPS Load (% per Phase)</td>
<td></td>
</tr>
</tbody>
</table>

### Automatic Battery Test
- The UPS shall initiate an automatic battery testing sequence periodically (default setting once a month), at a programmed day and time of day, selectable by the end user. It shall be possible for the user to disable the automatic battery test.
- Should a fault with the battery be detected, the UPS will immediately return to normal mode and a fault status (visual, audible, and remote) shall be indicated. No audible or remote signal indication of the battery test shall be communicated during the duration of the automatic battery test.
- The automatic battery test shall operate if no UPS alarm conditions are present and if the battery is at least 90% of its full capacity.

### Remote Emergency Power Off (EPO)
- The remote 'emergency power off' function (EPO) shall allow the user to immediately shutdown the UPS output supply in an emergency situation. The EPO shall be able to interface with normally closed, volt-free contacts external to the UPS. The EPO connection to the UPS shall be to a clearly identified terminal block type connector.
- The UPS EPO shutdown function shall not operate if the UPS internal manual bypass switch is in the bypass position. When the external EPO function has been re-set, manual intervention is required to restart the UPS. The electrical contractor shall include the facility for interfacing the EPO circuit with the supply feed of the UPS and provide a means of disconnecting all sources of power to the UPS.

### Standby Generator On contact
- The UPS shall have the facility whereby, on receipt of a volt free contact closure start signal from a standby generator supplying the UPS, the UPS system will automatically:
  - Inhibit Battery Recharge (Selectable);
  - Inhibit Transfer To Bypass (Selectable).

### Bypass
- **General:**
  - A bypass circuit shall be provided as an integral part of the UPS.
  - The bypass control logic shall contain an automatic transfer control circuit that senses the status of the inverter logic signals and operating and alarm conditions. This control circuit shall provide a transfer of the load to the bypass source, without exceeding the transient limits specified herein, when an overload or malfunction occurs within the UPS.

- **Automatic Transfers:**
  - The transfer control logic shall automatically activate the bypass, transferring the critical AC load to the bypass source, after the transfer logic senses one of the following conditions:
    - Inverter Overload Capacity Exceeded;
    - Inverter Over Temperature;
    - UPS Fault Condition (Non Redundant Configuration).
  - For inverter overload conditions, the transfer control logic shall inhibit an automatic transfer of the critical load to the bypass source if one of the following conditions exists:
    - Inverter/Bypass Voltage Difference Exceeding Preset Limits (-20/+15 % of Nominal Load);
    - Bypass Frequency Out of Preset Limits (± 4 % of Nominal Frequency).

- **Automatic Retransfer:**
Retransfer of the critical AC load from the bypass source to the inverter output shall be automatically initiated unless inhibited by manual control. The transfer control logic shall inhibit an automatic retransfer of the critical load to the inverter if one of the following conditions exists:

- Bypass Out-Of-Synchronization Range with Inverter Output;
- Overload Condition Exists in Excess of Inverter Full Load Rating;
- UPS Fault Condition Present (Non Redundant Configuration).

**Manual Transfer**:
In addition to the internal static bypass switch, the UPS shall have an internal manual bypass ‘make-before-break’ transfer switch. The manual bypass function shall be provided via a switch, which is accessible from the front of the UPS and located behind the UPS cabinet door. The manual bypass switch shall be electrically interlocked to prevent back-feeding the UPS output in the event of incorrect operation, e.g. transferring the load to bypass via the manual bypass switch when the load ids supplied by the inverter.

The UPS shall initiate an audible alarm upon transfer to manual bypass. The audible alarm shall be capable of being muted by the user. The alarm shall continue to sound (unless muted) while in bypass mode. This shall provide a reminder to the user that the load continues to be powered from utility or generator supply alone.

**Battery**:
The battery system shall consist of gas recombination, valve regulated, lead acid cells, compliant with BS6290 Part 4 and BS EN6089-2. Flame retardant batteries shall be provided, which renders the UPS suitable for installation inside a computer room.

The UPS battery charging circuit shall comprise of a separate battery charger and not depend on a charge voltage being derived from the UPS input rectifier. Consequently the battery charging voltage shall have zero AC (ripple) content.

For single UPS systems the battery system shall consist of a minimum of 2 parallel strings of multiple cells. Each individual parallel string shall have its own dedicated means of electrical protection.

For multiple UPS units connected in parallel the battery system shall be either:

- A common battery feeding all the UPS units. In this case the battery system shall consist of a minimum of 2 parallel strings of multiple cells. Each individual string shall have its own dedicated means of electrical circuit protection.
- A separate battery system for each individual UPS unit. In this case each separate battery system may consist of one protected string of multiple cells. If two or more parallel strings are used then each individual string shall have its own dedicated means of electrical circuit protection.

For all the above battery system arrangements the batteries shall be configured so that in the event of a battery malfunction the affected string is automatically isolated from the system thereby ensuring battery autonomy is retained (see System Description 1.4.18.2).

**1.4.28.3 COMMUNICATIONS**

The UPS shall incorporate voltage-free relay contacts suitable for direct communication with either a computer system, remote alarm panel or the clients BMS system and an RS-232 communication port for serial communications and to enable communication via modem equipment.

(a) **Relay Contacts**:

- The Relay Contacts shall be available through one DB-25F Communication Connector. The UPS shall communicate, via Volt-Free Relay Changeover Contacts, the following Status Signals:
Pin 1: Mains Failure (Normally Open);
Pin 2: Mains Failure (Normally Closed);
Pin 4: Load on Inverter (Normally Closed);
Pin 5: Load on Inverter (Normally Open);
Pin 7: Battery Low (Normally Open);
Pin 8: Battery Low (Normally Closed);
Pin 10: Load on Mains (Normally Open);
Pin 11: Load on Mains (Normally Closed);
Pin 13: Common Alarm (Normally Open);
Pin 14: Common Alarm (Normally Closed);
Pin 23: +12 VDC (Maximum 100ma);
Pin 22: GND.

(b) Serial Communications:
- The UPS shall have the facility for communication via an RS-232 port. The Pin-Out
  Configuration for RS 232 Port shall be as follows:
  Pin 2: Transmit Data;
  Pin 3: Receive Data;
  Pin 5: Common.

(c) Network Communications:
- The UPS unit(s) shall include a facility for installing an optional SNMP adapter card
to the UPS to permit one or more network management systems (NMS) to monitor
the UPS in TCP/IP network environments. 10/100 Mbit Ethernet support shall be
included.

(d) Parallel Operation:
- It shall be possible to configure the status signals from each UPS unit connected in
parallel to a common signal programmer device whereby, using Boolean logic,
input events or combinations of input events can trigger specified output signal
alarms and status events. It shall be possible to communicate the status of the
parallel UPS configuration over a LAN/WAN network via NMS and provide modem
communication to facilitate remote monitoring via a dedicated telephone line.

1.4.29 SCHEDULE OF PARTICULARS AND INFORMATION FROM
TENDERERS

ALL SCHEDULES WHICH ACCOMPANY THIS TENDER NOTICE FORM AN INTEGRAL PART OF IT
AND SHALL BE DULY COMPLETED IN EVERY DETAIL, FAILING WHICH THE TENDER IN
QUESTION MAY BE REJECTED.

Under no circumstances will statements such as the following be accepted by the
Client:

“See attached pamphlets”
“Refer to catalogue”
“Date to follow”
“As given by supplier, etc."

Equipment offered and listed in the Schedules shall be capable of performing the specified duties
and shall comply in all respect with the requirements of the specification.

Should it transpire that such equipment, even when offered by make, model and/or type, is
unsuitable of meeting or performing in accordance with the Specification requirement in any
respect, the Contractor or Subcontractor shall nevertheless be responsible for any additional costs
incurred in providing the required or suitable equipment.

Whenever a specific make, model or type of equipment has been prescribed in the Specification
and The Contractor offers an alternative or equal make or type of equipment in his tender, the
Client will, on acceptance of such a tender, inform the prospective Contractor in writing as to the make and/or type of equipment accepted. However, it should be noted that the use of words “OR EQUAL” by The Contractor is to be discouraged and could lead to the disqualification of the tender.

The Contractor will not be Allowed to supply Equipment other than that Offered in His Tender without the Written Approval of the Client.

1.4.30 USER DOCUMENTATION

The specified UPS system shall be supplied with three (3) user's manuals.

Manuals shall include :

(a) General Arrangement of the UPS Showing Dimensions and Weight;
(b) User Operating Instructions;
(c) Single Line Schematic Diagram with Functional Description of the Equipment;
(d) Installation Drawing along with Recommended Cable and Protective Device Sizes;
(e) Safety and Maintenance Guidelines.

1.4.31 AFTER SALES SERVICE

1.4.31.1 WARRANTY

The UPS manufacturer shall warrant the UPS system, including the batteries, against defects in materials and workmanship for 12 months from the date of commissioning or 15 months from the date of delivery, whichever is soonest. Subject to the UPS's being commissioned by the manufacturers trained engineer, the warranty shall provide free replacement parts and on-site labour.

1.4.31.2 EXTENDED WARRANTY

The UPS manufacturer shall provide the facility for enhancing or extending the warranty by providing an annual maintenance contract.

The Maintenance Contract shall provide :

(a) Guaranteed Response Time;
(b) Two Preventative Maintenance Visits per year;
(c) 24 Hour Telephone Support Directly from the UPS Manufacturer;
(d) Free Labour, Travelling to Site and Incurred Expenses;
(e) Free Replacement Parts (excluding Batteries outside the Warranty Period).
1.4.32 QUALITY ASSURANCE

1.4.32.1 UPS MANUFACTURER QUALIFICATIONS

The UPS manufacturer shall have a minimum of 10 year's experience in the design, manufacture, and testing of solid-state UPS systems.

1.4.32.2 FACTORY TESTING

Before shipment, the manufacturer shall fully and comprehensively test the system to assure compliance with the specification. These tests shall include full functional tests at the UPS rated load and a minimum 12 hour continuous burn in test at the UPS rated load.

1.4.33 GUARANTEE

(a) The Contractor will be required to guarantee the complete plant for a period of twelve (12) months from the date it has been taken over by the Client in running order.

(b) If during this period the plant is not in working order, or not working satisfactorily owing to the faulty material, design or workmanship, the Contractor will be notified and immediate steps shall be taken by him to rectify the defects and/or replace the affected parts on site, at his own expense.

1.4.34 MAINTENANCE

1.4.34.1 INITIAL MAINTENANCE

The Contractor will be required to maintain the plant in good running order for a period of twelve (12) months after the plant has been taken over by the Engineer. The cost of this maintenance shall be included in the tender price.

During this time, the Contractor shall undertake to arrange a three monthly visit to the plant by a qualified member of his staff, who shall:

Report to the Client keeping the Maintenance Records, and Enter into a Log Book the Date of the Visit, the Tests Carried Out, the Adjustments Made, and Any Further Details that may be Required.

When Necessary Clean the Plant and its Components.

Grease and Oil Moving Parts where Necessary.

Test-Run the Plant for half (½) an hour, Check the Automatic Starting with Simulated Faults on Each Mains Phase, and Check The Proper Working of All Parts, Including the Electrical Gear, the Protective Devices with Fault Indicators, the Change-Over Equipment and the Battery Charger. The Necessary Adjustments shall be made.

Report to the Client on Any Parts that become Unserviceable through Fair Wear And Tear, or Damaged beyond the Control of the Contractor.

The Contractor shall along with the report immediately submit a detailed quotation for the repair or replacement of such parts to the Client.

The Contractor may be required to maintain the plant in good running order for a period of forty eight (48) months after the original twelve (12) month maintenance period has expired. The full costs of this maintenance shall be included in the tender price, inclusive of overhead and travelling fees. A part from the consumables as detailed below, the Client shall not acknowledge any cost claims additional to this maintenance cost as tendered.

This agreement may initially be for twelve (12) months and visits shall take place at three (3) monthly intervals. The agreement may subsequently be renewed on an annual basis.
However, should the Contractor fail to hand over the plant in good working order on expiry of the specified twelve (12) months, the Contractor will be responsible for further monthly maintenance until final delivery is taken.

**Failing to submit a maintenance price will result in the tender being summarily disqualified.**

### 1.4.34.1.1 MAINTENANCE TOOLS

(a) The Contractor shall provide one set of all special tools, panel keys, etc., required for testing, maintaining and operating of all items of equipment.

(b) Duplicate keys shall be provided for all control panels, instrument locks, etc.

### 1.4.34.1.2 AVAILABILITY OF SPARES

(a) Spares and replacement parts shall be readily available in the Republic of South Africa and a guarantee of availability for a period of ten years shall be furnished.

(b) The Contractor shall submit a priced schedule of recommended spare parts, which should be carried on site.

### 1.4.34.1.3 INSTRUCTION OF OPERATOR

On completion of all tests, to the satisfaction of the Engineer, the Contractor shall continue to be responsible for the complete operation and maintenance of the plant for a period of three weeks during which time instructions shall be given to the Client's staff of the proper operation and maintenance of the plant, until he is fully conversant with the equipment and the handling thereof. The cost for such training shall be included in the tender price.

The operation and maintenance of the plant, for the duration of the instruction period, shall not in any way relieve the Contractor of his responsibility under the terms of the Contract.

Three copies of a Maintenance, Fault-Locating and Operating Manual are to be handed over the Client's representatives on site together with the Drawings specified above.

### 1.4.35 OPERATING AND MAINTENANCE MANUALS

The Contractor shall provide three (3) copies of the Operating and Maintenance Manuals.

The Contractor shall submit, for approval to the Engineer, four (4) weeks before completion of the installation, one (1) copy of the maintenance and operating manuals for the system supplied.

The Engineer will return these to the Contractor, within ten (10) working days of their receipt by him, marked with all changes, which are necessary.

The Contractor shall modify the manuals, as required by the Engineer and submit to the Engineer, within ten (10) working days, one (1) revised copy of the manuals. On completion of the installation, but before the plant is handed over to the Client; the Contractor shall provide three (3) copies of the Final Operating and Maintenance Manuals for the system supplied. The manuals shall be bound in book form with hard plastic covers to withstand constant use.

The Manuals shall be Properly Indexed to Facilitate Easy Reference.

The Manuals shall Include:

- A List of Recommended Servicing Tools and Specialist Equipment;
- A List of Spares to be Supplied by the Contractor to Cover the Period of Warranty. The Spares to be Supplied during the Warranty Period will However not be Limited to the Listed Items;
A Priced List of Recommended Spares Necessary for a Period of four (4) Years of Operation;
Exploded Drawings for detailed spares list from which every item of Every Piece of Equipment can be Positively Identified for Ordering Replacements;
A List giving the Name and Address of the Local Agent for each Item of Equipment;
A List giving the Name and Address of the Manufacturer of Each Item of Equipment;
Originals of All Test Certificates Obtained with the System;
A Preventative Maintenance Programme for All Equipment;
Operating Instructions for Each Item of Equipment;
Performance Data and/or Characteristic Curves;
Commissioning Data;
Record Drawings.

1.4.36 TESTS

The following tests are to be carried out:

(a) At the supplier’s premises, before the UPS will be delivered to site Representatives of the Client may be present during the test to satisfy themselves that the UPS complies with the specification and delivers the specified output.
(b) These test may also be carried out on Site if so requested by either the Engineer or the Representative appointed by the Client.
(c) The Engineer shall be Timeously Advised of the date of the Test [Two (2) weeks Advance Notice].
(d) The load resistance and all instruments (test facilities, instruments, dummy loads and switchgear) which may be required for the tests have to be provided by The Contractor.
(e) On completion of the tests, a full test report shall be issued. The report shall contain all measurements taken.
(f) For both tests at the Manufacturer’s Premises and on Site, The Contractor shall prove all specified values contained in this document and issued in his own specifications and literature.
2 PHYSICAL SECURITY INFORMATION MANAGEMENT (PSIM) SYSTEM

AC

BMS

CCTV

DVR / NVR

FAT

FDS

HMI

IDS

PSIM

SAT

SMS

SOC

SOP

VMS

Access Control System

Building Management System

Closed Circuit Television System

Digital Video Recorder / Network Video Recorder

Factory Acceptance Test

Functional Design Specification

Human Machine Interface

Intrusion Detection System

Physical Security Information Management

Site Acceptance Test

Security Management System

Security Operations Centre

Standard Operating Procedure

Video Management System

2.1 PSIM OVERVIEW

Physical Security Information Management (PSIM) Software enables Security Departments to manage an enterprise’s exposure to security risk. It is designed to aid decision making and deployment planning within an organization.

Within physical security operations it has been widely accepted that critical information from numerous sources is left to system operators to interpret and act upon consistently and correctly. Most end users have video surveillance, access control and building management systems. These systems are not integrated together and work independently with no communicating with other systems in the ecosystem.

PSIM does not just provide an integrated user interface, by providing a common operating platform, where multiple disparate systems are consolidated, intelligence is applied through workflow process management;

2.2 MANDATORY REQUIREMENTS

The PSIM solution shall be a software product that provides a platform and applications designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.

The PSIM software shall be based on SOA Architecture with the ability to distribute alarm and event processing services onto multiple servers. It shall also be possible to install the software in a Windows Failover Cluster for increased availability. The PSIM solution shall support increased alarm and event handling by adding multiple servers to the solution.

The PSIM solution shall integrate a wide range of security products including Video Management Systems (VMS), Security Management Systems (SMS) [Access Control], IP Intercoms (IP PBX) and Intruder Alarm System (IDMS). The PSIM solution shall be capable of receiving events form integrated systems and execute functions on the systems.

The PSIM solution shall incorporate means to implement business security processes through automatic workflows and visual process guidance. It shall be possible to change the workflows and process guidance without upgrading the software or restarting the solution.

It shall be possible to configure the Process Guidance so that the relevant information is provided to the users, increasing the situational awareness while resolving incidents.
The PSIM solution shall include static and interactive map capability including the display of alarm locations, data layers, camera asset locations. High resolution image files shall be supported and automatically be cached to improve the overall user experience. It shall be possible to display maps from ESRI ArcGIS and any WMS compatible map data sources.

The PSIM solution shall provide a video review interface for display of live and recorded video from connected Video Management Systems. The interface shall be unified and consistent regardless of the underlying video system and be capable of displaying video from different types of systems at the same time. It shall provide functionality for viewing live video, recorded video, saving snapshots, viewing video in full screen, pan-tilt-zoom control and preset functions.

The PSIM Solution shall contain a dedicated feature for exporting video. The feature shall allow the capture of all related video for an incident regardless of sub-system type or combination of sub-systems providing the video for the location where the incident occurred. The exported video shall be stored on a configured network share and it shall be possible to generate a report describing what video has been exported.

The PSIM solution shall have a configurable end-user interface. It shall be possible to build new interfaces and configure interfaces to display different content depending on the situation and operator. It shall be possible to create and update user interfaces without upgrading the software or restarting the application.

The solution shall have the ability to use COTS reporting tools such as Microsoft SQL Server Reporting Services to generate reports on data collected and generated by the PSIM solution. It shall be possible to generate these reports automatically or as a result of an event. It shall be possible to preview reports in the operator user interface before generation. It shall be possible to automatically generate and email reports on a regular basis or as a result of an event.

The solution shall contain user interface components for the creation of live Dashboards. Dashboards components shall include Bar Charts and Graphs, RSS readers, Media players, Labels and Web Browsers. It shall be possible to link the Dashboard indicators to data sources and the indicators shall update when the data changes.

The PSIM solution shall allow for granular permissions control for users and user groups and include permission inheritance. Areas that it shall be possible to restrict through permission configuration shall include: Alarm visibility, access to physical locations, and visibility of CCTV assets, video playback control, and Pan-Tilt-Zoom (PTZ) priority.

The PSIM solution shall provide functionality to connect to new and existing data sources and present this data to operators using the solution. It shall be possible to create, read update and delete data from these sources form workflows defined in the solution.

The PSIM solution shall include an easy-to-use administration interface containing functionality for managing users and groups, viewing device states, managing locations and asset locations on maps.

The PSIM solution shall be designed to run on Server 2012 or later, Windows 7 and Windows 8.1 or later for workstations. It shall support Windows Failover clustering and be built using the latest Microsoft .Net framework.

The PSIM solution shall support Federation - Using Federation, multiple independently administered same vendor PSIM systems can connect to each other and share resources. A trust relationship is configured between the PSIM Sites, ensuring that users from each system will be able to access, control and receive events from the remote systems assets.

The PSIM solution shall support a Device Driver Kit as standard, the device driver interface enables 3rd parties to write drivers which is flexible and scalable according to the need.

The PSIM solution shall support a Video Streaming Service and have the ability to stream video from any sub system in a common format such as H.264 and distribute using standard streaming techniques such as RTSP or HLS.
The PSIM solution shall support a Centralised Video Export facility – with an Intuitive interface, to export incident video from multiple sources in both an industry standard format, and the native recording format.

The PSIM solution shall support a Customisable User Interface, allowing trained, certified engineers to build, commission, and customise user interfaces in real-time.

The PSIM solution shall include video wall tools that turn any screen into a dynamic video wall.

The PSIM solution shall include a Workflow Engine, which when using the response plan editor, creating custom logic and workflows based around the customers’ business process without changing the core build.

The PSIM solution shall be able to integrate any Sub-System, not just those that are traditionally related to Security.

2.3 FUTURE CAPABILITIES

Supplier must demonstrate that the PSIM solution is being continually developed and enhanced according to market requirements, industry and technological advances.

2.4 QUALITY ASSURANCE

The manufacturer shall have a minimum of eight (8) years’ experience in the production of PSIM software products.

2.5 PRODUCT

2.5.1 SOFTWARE COMPONENTS

The PSIM solution shall be comprised of a number of software services that shall operate independently, allowing the solution to be scaled onto separate servers per service as required.

All services shall be able to automatically restart so no single component can inhibit the entire system operation.

It shall be possible to backup and restore databases.

2.5.2 DEVICE ASSETS

The PSIM Solution shall include features to represent devices data points as logical assets. Example data points are Access Control Doors, CCTV Cameras, IP Intercoms, or Intruder Alarm Sensors.

It shall be possible to visualize assets on maps.

2.5.3 ALARM MANAGEMENT

An Alarm Type feature shall be included in the PSIM Solution, allowing users to define Alarm types. An Alarm Type is identified by a combination of metadata and defines system behaviour when then Alarm Type is activated.

The PSIM Solution shall include an Alarm Stack feature that shows Active Alarms. Multiple alarm stacks should be possible, allowing individual control.

Each Alarm Type shall have configurable fields, such as description, priority and Icon.

It shall be possible to configure an Alarm Type to become active depending on a number of different parameters such as event type, location or value.

It shall be possible to override the alarm description visible to the user by concatenating Alarm data.
It shall be possible to configure a Schedule for each Alarm Type so that alarms of the type only become active if the event(s) activating the alarm is/are received during the scheduled time. It shall be possible to configure an Alarm Type to be a Manual Alarm. A Manual Alarm shall not require an event from an edge system in order to activate the Alarm. It shall be possible to initiate the alarm from a workflow. It shall be possible to identify an Alarm Point for each alarm activation. It shall be possible to configure the Alarm Type so that Alarm Points are identified by:
- The Event Originator;
- The Value of One of the Properties of the Event;
- The Value of One of the Properties of the Event in conjunction with a Placeholder Configured in the Solution.
It shall be possible to collate alarms so that multiple events are linked to the same alarm rather than activating multiple alarms. It shall be possible to initiate workflows when an alarm is activated, or handled by an operator. It shall be possible to define and save alert state formatting to apply to specific assets. It shall be possible to initiate alert state formatting for a specific asset when it is identified as an alarm point for an alarm. It shall be possible to change the visual appearance indefinitely or for a specified period of time.
The PSIM Solution shall have a built-in way of managing Service Level Agreements associated with different Alarm Types. It shall be possible to configure default behaviour for 3 Service Levels. It shall be possible to configure each Alarm Type so that it adheres to the default Service Level configuration, a specific configuration for the Service Level for the Alarm Type or for no Service Level to be monitored. It shall be possible to associate a Resolution Type with an alarm when it is closed. It shall be possible to configure available Alarm Resolution Types. It shall be possible to associate alarm activities with an alarm. It shall be possible to configure available Alarm Activities. It shall be possible to associate Alarm Activities with an alarm from a workflow.
The PSIM solution shall include a Threat Level Indicator which can show the current state of threat. The Threat Level Indicator shall be configurable so that a range of different colours can be used and threat level descriptions. It shall be possible to change the threat level from a workflow. It shall be possible to consolidate sensors into Asset Groups (for example Fire Doors) so response plans can be triggered from Asset group opposed to individual devices. It shall be possible to Schedule Alarm stacks to only show within a predetermined window of time, allowing satellite control rooms to only receive alarms during a set period, and any time outside of the agreed schedule, the central control room will receive all events.

2.5.4 TRIGGERS

The PSIM Solution shall include a Trigger feature that can be used to link incoming events to workflows. It shall be possible to prevent Triggers from activating for a specified time after an event is received. It shall be possible to specify a specific event that shall activate the Trigger. It shall be possible to specify that any event from a specific type of device shall activate the Trigger. It shall be possible to specify that the Trigger should only be activated when specific conditions in the event data are met. It shall be possible to initiate a Workflow, passing all the data from the event to the Workflow variables.
2.5.5 ALARM STACK

Active Alarms shall be visible in a built-in alarm stack.
It shall be possible to configure multiple alarm stacks in one user interface.
It shall be possible to make one or multiple views on alarms available in an Alarm Stack depending on User and/or User Group membership.
For each Alarm Stack View, it shall be possible to apply various filters to change the priority of the information being displayed.
Alarm shall appear in the Alarm Stack in priority order based on the priority assigned to the Alarm Type.
The PSIM shall have the ability to filter alarm types, and provide the number of new alarm counts within the Alarm Stack View (Preventing multiple alarms from same system devices being missed).

2.5.6 DASHBOARD

The PSIM Solution shall contain a Chart component that can be included in one or multiple instances in one or many user interfaces.
It shall be possible to link the chart component to a pre-configured data source.
It shall be possible to configure one or many series of data.
The Chart component shall allow the display of data using different chart formats such as Pie, Bar.
The PSIM Solution shall contain a Gauge component that can be included in one or multiple instances in one or many user interfaces. It shall be possible to bind the Gauge control to a pre-defined data source.
It shall be possible to change the value range of the Gauge component.
It shall be possible to show the current value in a numeric indicator overlaid on the Gauge.
The PSIM Solution shall contain a RSS Reader component that can be included in one or multiple instances in one or many user interfaces.

2.5.7 MAP FUNCTIONALITY

The PSIM Solution shall include a Location object type.
It shall be possible to create, update and delete Locations.
It shall be possible to make one or many Locations sub-locations to other Locations so that for instance 1st Floor is a sub-location to Building A which is a sub-location to Campus A.
It shall be possible to associate a Location with a static image map, this shall support large high resolution images in-excess of 1.5GB, allowing seamless panning and zooming to specific areas of any map layer.
It shall be possible to save the Latitude and Longitude for a Location.
It shall be possible to add Security Assets to a Location.
It shall be possible to create shortcuts to Security Assets and add these shortcuts to a Location so that a Security Asset can be associated with multiple Locations.
It shall be possible to display a Static Image Map associated with a Location to the user.
The solution shall support jpg/jpeg, gif and png image files.
It shall be possible to display an Open Street Map to the end user.
It shall be possible to display a WMS / WMTS compatible map to the end user, this includes maps served over WMS/WMTS by:
- Esri ArcGIS;
- GeoServer.
The user shall be able to pan and zoom any map.
It shall be possible to configure which icon to use for each individual asset plotted on a map.
It shall be possible configure a custom user interface to be displayed when the user selects an object on the map.
It shall be possible to configure a custom text to be displayed for assets shown on maps.
It shall be possible to display lens projection on static maps, illustrating the angle to which the camera is pointing
The system shall display video from a camera when the user selects the camera on a map and drops it on a display tile or a video wall drop zone control
It shall be possible to configure additional WMS/WMTS layers
WMS/WMTS maps shall support KML/KMZ Layers
The map shall feature a Layer Tree where the user can select which layers to show when using a map that supports Layers.
It shall be possible to track geographically aware Assets automatically on the map.
It shall be possible to search the current map for assets within that map layer.

2.5.8 VIDEO DISPLAY

The PSIM solution must be capable of simultaneously displaying multiple video streams on a single display, including but not limited to 4, 6, 9 and 16 tile layouts. These live or recorded video streams can be from disparate analogue and digital sources, including those from different manufacturers, all displayed concurrently.
Clicking on a video tile should bring up a tool menu that allows all available functions to be presented to a correctly authorized operator. The menu should have the following buttons subject to user permissions and VMS capability:
• Full Screen;
• Still Image Snapshot;
• Toggle Video Playback Mode;
• PTZ Preset Control;
• Toggle PTZ Lock.

2.5.9 VIDEO PLAYBACK

It shall be possible to toggle the video display mode form live to playback by pressing the playback button in the video display toolbar.
It shall be possible to toggle individual video tiles into playback mode independent of each other.
The PSIM user interface shall be able to playback or show live, or any combination of the two, multiple video cameras across multiple VMS systems and manufacturers simultaneously to the operator, with no practicable limit imposed from the PSIM software on the number concurrently controlled.
The playback control shall be the same (subject to user permissions and VMS capability) independent of the underlying Video Management System.
When supported by the VMS the playback mode shall display a time bar showing available video footage chunks
A fixed timeline with a continuous chunk should be displayed in the time bar when the accessed Video Management System does not support querying for available storage chunks
The playback interface shall offer the following functionality to the user (subject to user permissions and VMS capability):
• Go to time by clicking in a time bar;
• Go to time by selecting date form a calendar and time from a time control;
• Playback speed;
• Play/Pause.

2.5.10 VIDEO DISPLAY PERMISSIONS

All playback, PTZ and live view functionality must integrate with the PSIM permissions engine. It must be possible for the PSIM to restrict any of the individual actions based on user login and role. These permissions must be definable in one location and must be applied to all types of VMS manufacturer integrated into the solution.
2.5.11 VIDEO DISPLAY SEQUENCES

The PSIM solution shall offer the user the ability to create display sequences of cameras from a mixed range of video management systems. It shall be possible to define the dwell time, preset position and user access for the sequence. The PSIM Solution shall include a Wizard assisting the user in creating new Sequences. It shall be possible to add a Location to one of the Sequence steps. This will display all camera in the selected Location. It shall be possible to save a sequence for the current user or for sharing with other users. When displaying a sequence it shall be possible to pause, step back and step forward. It shall be possible to display a sequence on a video wall by dropping it on a Video Wall Drop Zone Control.

2.5.12 VIDEO DISPLAY TILE LAYOUTS

The PSIM solution shall offer the user the ability to create video layouts with content from multiple sub-systems. It shall be possible to save personal layouts or share layouts with multiple users. It shall be possible to configure which tile layout types are available to the end user when creating new tile layouts. The following Tile Layout definitions shall be included in the solution by default:

- 1-Way
- 4-Way
- 6-Way
- 6-Way 1-Hotspot
- 9-Way
- 16-Way
- 16-Way 2-Hotspot
- 16-Way 1-Hotspot
- 16-Way 1-Centered Hotspot
- 16-Way 3-Hotspot
- 9-Way 1-Stretched Hotspot
- 9-Way 1-Hotspot
- 25-Way 1-Hotspot
- 36-Way 1-Hotspot
- 64-Way 1-Hotspot
- 6-Way (Wide)
- 8-Way (Wide)
- 12-Way (Wide)
- 12-Way 1-Hotspot (Wide)
- 12-Way 2-Hotspot (Wide)
- 12-Way 1-Stretched Hotspot (Wide)
- 20-Way (Wide)
- 20-Way 1-Hotspot (Wide)
- 20-Way 1-Centered Hotspot (Wide)

It shall be possible to define custom tile layout definitions. It shall be possible to display a saved Tile Layout on a video wall by dragging and dropping it on a video wall drop zone control. It shall be possible to save a Tile Layout in a Location.

2.5.13 PAN TILT ZOOM CONTROL

It shall be possible to control Pan and Tilt of a connected, integrated camera by clicking in the video image and moving the mouse.
It shall be possible to zoom in and out by using the mouse wheel
It shall be possible to call stored preset positions from the video display menu
It shall be possible to store the currently viewed angle as a preset position
It shall be possible to control Pan, Tilt and Zoom using a connected DirectX (DirectPlay) Joystick such as the Axis T8310. When using a connected compatible Joystick, PTZ control shall not be limited to video feeds from video systems compatible with the Joystick manufacturer.

2.5.14 VIDEO EXPORT

The PSIM Solution shall contain a dedicated feature for exporting video from integrated sub-systems
It shall be possible to create an export Job, containing export tasks from multiple cameras connected to multiple video systems
It shall be possible to combine video sources from different model and makes of video systems into the same export job
The solution shall automatically schedule export jobs of video based on:
- Number of maximum connections to the Location where the VMS is located
- Number of maximum connections to the VMS
- Number of Maximum concurrent exports
It shall be possible to password protect video exports.
It shall be possible to schedule a job from a workflow
It shall be possible to manually schedule a job by using a built-in Video Export Wizard
The system shall estimate the total size of the exported video footage when a job is manually scheduled and display this to the user before the job is saved
The system shall estimate the total duration it will take to export all video in the job when a job is manually scheduled and display this to the user before the job is saved
It shall be possible to list active jobs for the current user
It shall be possible to list active jobs for all users (subject to permissions)
It shall be possible to list completed jobs for the current user
It shall be possible to list completed jobs for all users (subject to permissions)
It shall be possible to configure where video can be exported to
It shall be possible to configure:
- A size limit at which to warn the user when scheduling a new job
- A maximum size limit at which to prevent the user from scheduling a job
- A duration limit at which to warn the user when scheduling a new job
- A maximum duration limit at which to prevent the user from scheduling a job
It shall be possible to automatically generate a pdf report when a job has completed and store in the export location
The system shall notify the user when a job scheduled by the user has been completed
It shall be possible to prioritize a job so that it is executed before other scheduled jobs (subject to permission)
2.5.15 VIDEO WALL DISPLAY

The PSIM Solution shall include a video wall feature, allowing dedicated client workstations connected to multiple large screens to be used as Video Walls.

It shall be possible to configure which client work stations to use as Video Walls.

The PSIM Solution shall contain a user interface control representing one or multiple video wall displays, the Video Wall Drop Zone control.

The Video Wall Drop Zone control shall allow the user to drop content on the control for it to be displayed on the Video Wall Client.

It shall be possible to close the content on a video wall tile by clicking a close button on the drop zone control.

It shall be possible to configure the drop zone control so that it shows the name of the camera that is currently being shown on the video wall.

It shall be possible to configure one or many Tile Layouts to use on the Video Wall and Drop Zone control.

It shall be possible to change Tile Layout on the video wall from the Drop Zone control, either by "Drag and Drop" or from user selection.

The PSIM Solution shall include a Leasing feature, preventing control of a single video wall by multiple users.

It shall be possible to display Graphical User Interfaces on the Video Wall by dropping them onto the drop zone control.

It shall be possible to display camera feeds on the Video Wall by dropping them onto the drop zone control.

It shall be possible to display Sequences on the Video Wall by dropping them onto the drop zone control.

It shall be possible to use the Drop Zone control to integrate with 3rd party Video Wall controllers such as Barco CMS.

2.5.16 CONTACTS AND CONTACT GROUPS

It shall be possible to define contacts in the PSIM Solution.

It shall be possible to associate a contact with a Location.

It shall be possible to view Contacts for a Location in the end-user interface.

It shall be possible to create groups of Contacts.

2.5.17 DATA ACCESS

The PSIM Solution shall include a feature which allows configuration of data access from external sources, Data Connections.

Data Connections shall be able to use OLE DB Providers installed on the server running the Core Server component.

Data Connections shall be able to use ODBC DSN's configured on the server running the Core Server component.

It shall be possible to configure a Data Connection to use Windows Integrated Security or a username and password.

It shall be possible to test the connection before saving.

It shall be possible to configure the Server or filename to access or to select to access a database local to the server where the Core Service is running.

The Data Connection should display available tables and views once the connection properties have been configured.

It shall be possible to retrieve data from tables through the Data Connection configuration interface.

It shall be possible to configure customized Views on the data available through a data connection.
It shall be possible to configure columns to appear as link labels
It shall be possible to configure the view to show a progress bar panel when a link label is clicked
It shall be possible to configure the following for each individual column in a view
  • Date Format
  • Header Text
  • Lookup Column
  • To show a check box for True/False values
  • If the column is visible
It shall be possible to configure a column so that an icon is displayed instead of a text and the icon is selected based on the value in the column
It shall be possible to configure the view to use a different back and fore color depending on the value in a column (conditional row formatting)
The PSIM Solution’s workflow engine shall contain functions that can use Data Connections to:
  • Insert Data;
  • Select Data;
  • Update Data;
  • Delete Data.

2.5.18 REPORTING SERVICES

It shall be possible to use standard business reporting tools such as Microsoft SQL Reporting Services (SSRS) to create custom reports using data generated by the PSIM solution.
It shall be possible for the End user or system integrator to create custom reports without the need for development support, providing the appropriate knowledge transfer has been undertaken.
It shall be possible to generate reports based on report templates stored in SSRS from the workflow engine.
It shall be possible to preview reports generated using report templates stored in SSRS in the PSIM Solutions graphical user interface.
It shall be possible to configure the SSRS service connection details in the PSIM Solution.

2.5.19 SCALABILITY ARCHITECTURE

It must be possible to install the PSIM server services onto multiple servers (nodes).
It shall be possible to distribute sub-functionality, such as reporting to separate, dedicated hardware so that the overall solution can handle a greater load.
It shall be possible to deploy multiple instances of the Event service in order to process more events per second
It shall be possible to deploy multiple instances of the Rules Engine service in order to evaluate more Alarm Types per second
A Shared SQL Storage (SAN) for the SQL database is required where redundant operation is required, it is recommended that the SQL database is deployed using RAID 10.

2.5.20 VIRTUALISATION ARCHITECTURE

It shall be possible to deploy the PSIM servers and Storage in a Virtualisation environment.
Vendors such as VMware vSphere and Microsoft Hyper V shall be supported, and capable of being deployed in a High Availability mode of operation.
When deploying Virtualisation, there should not be a host OS installed for the Hypervisor layer.
When Virtualisation is used, the minimum specification of Server hardware shall mirror that of the Physical recommended specification, especially in respect of storage and CPU Quantities.
The End User or Partner are responsible for employing the use of a Virtual Solution System Architect to design the required environment.

2.5.21 FEDERATION

It shall be possible to deploy a Site to Site federation.
In Federation it shall be possible to sync alarms from the sender to the receiver and allow users on the receiver to handle and resolve alarms from the sender.
In Federation it shall be possible to sync devices from the sender to the receiver to allow users at the receiver site to be able to view video (live and playback) whilst handling an alarm.
In Federation it shall be possible to sync schematic scenes from the server to the receiver, together with any map decoration, so that users at the receiver site can view location maps whilst handling an alarm.

2.5.22 FAILOVER ARCHITECTURE AND HIGH AVAILABILITY

It shall be possible to deploy the PSIM Solution in a Windows Failover Cluster.
When deployed in a Windows Failover Cluster, the core service shall automatically start up on a failover node should the primary node become unavailable.
The client application must automatically sign into an available backup server without disrupting the videos being displayed to the operator should a server fail.
The PSIM must support SQL replication to a disaster recovery environment.

2.5.23 EMAIL

The PSIM Solution shall provide functionality to send email over SMTP.
It shall be possible to send emails from workflows.
It shall be possible to send emails with attachments.

2.5.24 SNMP

The PSIM Solution shall provide functionality to broadcast SNMP messages from the proposed system.
Service State, Device State and Response Plan shape changes shall be broadcast.

2.5.25 WORKFLOW

The PSIM Solution shall contain a workflow engine and built-in workflow designer.
The Workflow Designer shall allow users to build workflows by adding and connecting pre-defined shapes in order of execution.
Each shape shall represent a set of functionality.
Each shape shall have a set of parameters that the user can define, for example, the Wait shape shall require the user to enter the time to wait.
The following shapes shall be available in the Workflow Designer:

- Action
- Add Member to Group
- Add to List
- Assign Variable
- Audit Log
- Authenticate Client
- Clear Collection
- Clear Tile Contents
- Close UI
- Configure Tile Layout
- Copy Object
- Copy Variable
- Create Alarm
- Data Delete
- Data Exec
- Data Insert
- Data Modifier
- Data Modifier
- Data Sync
- Data Update
- Delete Object
- Display Object
- Display Tile Layout
- Dynamic Action
- Dynamic Link
- Evaluate
- Export Media
- Finish
- Generate External Report
- Generate Report
- Generate Tile
- Geographical Query
- Get Group Members
- Get Groups for Member
- Get KeyMap from Object
- Get Location
- Get Object for Shortcut
- Get Object from KeyMap
- Get Placeholder
- Get Shortcuts
- Get Tile Contents
- Get Tile Contents from Client
- Go Sub
- Import Media
- Iterate Collection
- Join
- Label
- Link
- Log Activity
- Modify Alarm
- Move Object
- Obtain Lock
- Park Alarm
- Read Alarm
- Read Event Property
- Release Lock
- Remove from List
- Remove Member from Group
- Remove Tile Layout
- Resolve Alarm
- Schedule
- Script
- Search
- Select
- Set Tile Contents
- Split
• Start
• Submit Video Export Job
• Suppress Alarm Point
• Swap Tiles
• Tile Action
• Unsuppress Alarm Point
• User in Group
• Wait

The Workflow Designer shall allow users to create variables to store global data, data for the workflow and data from event initiating the Workflow.

A Shape shall have one or more outward routes (arrows) attached with the exception of the Finish shape.

The workflow designer shall allow for the connection of outward routes to other shapes thus establishing a flow of execution through the plan.

A Shape can have any number of routes entering it with the exception of the Start shape that can have no routes enter it.

The workflow designer shall allow for the modification of shape text to provide a more meaningful explanation of shapes purpose.

2.5.26 SUB-SYSTEM INTEGRATION

The PSIM shall be capable of receiving and transmitting information and events to and from integrated systems such as the Video Management systems (VMS), Security Management Systems (SMS) [Access Control], Intrusion Detection Management Systems (IDMS) and IP Intercom Systems (IP PBX).

The extent of the interaction between the PSIM system and the integrated sub-systems is dependent on the capability of the software development kit (SDK) or Application Programming Interface (API) supplied by each manufacturer of the integrated sub-systems.

Integrated sub-systems shall be implemented in stand-alone software packages that can be loaded by the core solution at run-time.

It shall be possible to add new integration packages after the core solution has been deployed.

The PSIM Solution shall include a configuration interface where the user can install and update integration packages (The Driver Manager).

The Driver Manager shall display the manufacturer and product name that each loaded integration package is compatible with.

The PSIM solution shall provide a trigger mechanism allowing the PSIM application to react to events occurring on any object under the control of the PSIM.

The system shall allow bi-directional control of sub-systems such as Access control to facilitate an override on allowing access. In addition it will also cause this to be escalated to a supervisor under certain conditions.

The system shall also be able to generate calls to connected intercom, Fire PVA, VoIP Telephony and cellular systems.

Integration packages must be architecturally separate from the core server application to ensure that instabilities in the third party SDK do not affect the core PSIM server application. This is also extended to the PSIM client application and should be achieved by hosting video content in a fault tolerant output control component designed to isolate and manage any video exceptions.

The PSIM system must not be limited to the type of system that it can integrate, now or in future, this should be achieved by representing all assets under its control as objects. These objects shall be represented in a generic manner exposing a set of properties, events and functions to the PSIM application. The objects shall be self-describing to the PSIM application. Objects shall be provided for all real-world touch points and for PSIM, specific functionality (triggers, storage and playback, badge management, positioning information etc.).
The PSIM Solution must be able to display and manage all of the integrated systems from one location that is accessible from any of the PSIM client applications. This should be achieved from a system configuration screen giving access to all the objects under the control of the PSIM.

The PSIM Solution shall support direct integration to sub-systems as opposed to require middleware servers such as Field Server.

The PSIM solution shall feature interoperability with major DVR and NVR manufacturer recording equipment and applications.

The PSIM application shall expose a high level of functionality from NVRs

The PSIM application shall expose a high level of functionality from DVRs

The PSIM solution should be capable of exposing the high level of functionality from NVRs and DVRs including playback, image retrieval, alarm events and health status where supported by the SDK/API.

The PSIM shall allow full PTZ control (including camera functions such as presets and tours) for the video cameras.

It shall also be possible to drive telemetry using a mouse by clicking within the CCTV image displayed in the GUI.

2.5.27 INTEGRATION SDK

The PSIM Solution shall support a Software Development Kit (SDK) available allowing independent creation of integrations for the PSIM Solution.

The SDK shall include:
- User documentation
- Microsoft Visual Studio templates
- Test harness that the user can use to test integrations outside of the PSIM software.

There shall be a training program for the SDK
There shall be a certification process for new integrations.

2.5.28 AUDIT TRAILS

The PSIM system must provide an Auditing mechanism

The PSIM must allow for audit points to be inserted at any point in an alarm handing process. Each interaction the operator undertakes must be recordable. The PSIM must allow the alarm handling process to be matched to the implemented security operating procedure.

It should be possible to automatically audit the following events:
- Dropzone Control Object Dropped - An object was dropped on the Dropzone
- User Interface Load - A User Interface has been loaded
- User Interface Close - A User Interface has been closed
- Live Video Start - Viewing of live video has started
- Live Video Stop - Viewing of live video has stopped
- Live Video Snapshot - A snapshot has been taken
- Live Video View Requested - A request has been made to view a camera. The distinction between this and Start is that this event is audited regardless whether the live video can actually be displayed.
- Live Video Close Requested - A request has been made to close a camera
- User Membership Added - An object becomes a member of another object
- User Membership Removed - An object is no longer a member of another object
- Object Created - An object has been created
- Object Enabled - An object is now enabled
- Object Disabled - An object is now disabled
- Object Removed - An object was removed
- Permission Allow Added - An Allow permission has been set
- Permission Allow Removed - An Allow permission has been cleared
- Permission Deny Added - A Deny permission has been set
- Permission Deny Removed - A Deny permission has been cleared
2.5.29 USERS AND PERMISSIONS

The PSIM Solution shall include a User object type.
It shall be possible to configure an Expiration date for a user. Once a user expires, the user cannot log in.
It shall be possible to force the User to change password on next log in
It shall be possible to Reset a user from being locked out
It shall be possible to configure the Users:
• Username
• First Name
• Last Name
• Password
• Address/Contact Details
• Geographical Location
The PSIM Solution shall include a Group object type.
It shall be possible to disable a Group. When a Group is disabled, it’s permissions shall not apply to members

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
It shall be possible to configure a Group to become Enabled at a specific time/date
It shall be possible to configure a Group so that it is:
- Never disabled (unless manually disabled)
- Disabled 24 hours after being enabled
- Disabled 7 days after being enabled
- Disabled on a specific date at a specific time
It shall be possible to create new Users.
It shall be possible to create new Groups.
It shall be possible to make a User a member of any number of Groups
It shall be possible to make any number of Users a member of a specific Group
When a User is a member of more than one Group it shall acquire the permissions from both Groups
It shall be possible to associate a User or Group with one or many Security Assets and/or one or many Locations
It shall be possible to prevent users from seeing that specific assets or locations exists
It shall be possible to configure the following user permissions required for video assets:
- Export Video
- Connection Settings
It shall be possible to configure the following user permissions required for video assets:
- View Live CCTV Stream
- View Playback CCTV Stream
- PTZ Control
- PTZ Preset Recall
- PTZ Preset Setting
- Export Video
It shall be possible to provide Alarm Stack views to selected Users and/or Groups, making it possible to hide or show specific Alarm Types to specific Users
The PSIM solution shall provide a graphical user interface to allow system administrators to assign a user to a user group and a user group to a security resource.
The PSIM Solution shall provide a graphical user interface wizard to assist creating new users.
A super user (group administrator) should be able to manage the user permissions for the groups of users they administrate.
Security resources may also be grouped (e.g. a building or a single site) such that users have permission only to interact with resources in single or multiple groups.
The permissions the PSIM shall allow an administrator to configure are:
- Create a new user
- Delete a user
- Disable a user
- Create a new user authentication group
- Delete a user authentication group
- Disable an authentication group
- Add a user to the authentication group
- Remove a user from authentication group
- View users in authentication groups
- View authentication groups
- Add a camera to an authentication group
- Remove a camera from an authentication group
- View cameras in the authentication group
- Apply permissions to a camera for an authentication group
- View current permissions for an authentication group
- Reset permissions for an authentication group
User permissions shall be configurable and effective in real time with at most 60 seconds between change and impact taking effect.
It shall be possible to configure a connection to a Microsoft Active Directory in the PSIM Solution.
It shall be possible to make an Active Directory user group a member of a user group native to the solution. When an Active Directory user is a member of an AD group and the AD group is a member of the native solutions group, the AD user shall acquire the permissions as configured in the native group. It should be possible to configure the system for automatic sign-in using Active Directory user credentials (Single SignOn). The PSIM Solution shall include an Administrator user by default that cannot be deleted.

2.5.30 GRAPHICAL USER INTERFACES

The solution shall provide functionality to create tailored and bespoke user interfaces without any software changes or updates. The PSIM solution shall feature a built in Graphical User Interface (GUI) designer. The GUI Designer can be used to create user interfaces to be shown on the Operator Workstations running the client application. The GUI Designer shall feature rich support for scripting and built in Operational Policies allowing dynamic policy-based behaviours to be executed as a result of user interaction. The GUI Designer shall allow the creation of interfaces giving full control over the visualizations systems such as control room display wall technologies. The GUI Designer shall allow the creation of rich interfaces incorporating multiple content sources including but not limited to, maps and graphics, hotspot areas, standard Windows-compliant GUI elements such as buttons and toolbars, web page content, RSS feeds, incident and alarm stacks, video wall control, matrix switching control, Pan-Tilt-Zoom (PTZ) camera control, device and user status indicators and access to all live and recorded video and audio streams on the connected video devices. The interaction between the PSIM GUI’s and the display walls shall be seamless to the operator. It shall be possible to drag and drop live video streams for review on the PSIM and also to drag and drop live video streams onto a representation of the current wall configuration on the PSIM.

There shall be no limit on the number of GUI’s that can be configured in the PSIM. All GUI’s created via the PSIM shall be published and be available immediately (subject to users permissions) to all PSIM applications on the Operator Workstation. Each bidder shall include within their return of tender for the cost of the design, development and creation of the GUI to control the devices and applications selected and advised elsewhere. The PSIM shall be capable of supporting an unlimited number of Windows (and hence an unlimited number of physical monitors). Display windows shall be configurable in the following manner:

- Maximised or freely positioned
- Custom title text
- Sized to fit height or width of physical monitor
- Hidden when empty (to support popup windows)
- Bordered or borderless (to facilitate scenarios where the window border is not required – i.e. video walls)

Each window under the control of the PSIM shall be capable of hosting an unlimited number of Display Areas. Display Areas can be hosted in five positions within a window, top, right, bottom, left or fill. The windows shall support a tabbed docking engine capable of further arranging the Display Areas within the window dock positions. Display Areas shall be capable of hiding their tabs when they are the only content in a window dock position to allow content to be maximized to fill the window dock position. The Tile Layout object shall be provided to host content within grid arrangements. Content is defined as Device or GUI objects. Tile Layout objects can be hosted within Display Areas. Tile Layouts can be delivered to multiple Display Areas on disparate PSIM installations simultaneously.
It shall be possible to host multiple Tile Layouts within one Display Area. In this scenario the Display Area shall use a tabbed layout engine to automatically layout the available Tile Layouts.

The Tile Layout designer shall be used to configure Tile Layout objects. The Tile Layout designer shall provide a set of pre-configured grid arrangements and allow for the creation of custom grid arrangements. The designer will also allow for default content to be stored within the Tile Layout object.

The Tile Layout object shall expose properties for title overlays for individual Tiles. Title overlays will provide the following properties:

- Title font
- Foreground and background colour
- Visibility (always, only Devices, none)

When hosted within a Display Area the Tile Layout object shall provide the following end-user functionality:

- Clear contents (subject to permissions).
- Full Screen (if displaying a video Device).
- Instant Replay (if displaying an instant-replay capable Device).

The GUI Designer shall offer the user the following User Interface components to use when designing a User Interface:

- Button
- Checkbox
- Comments Box
- Data Navigator (To step between data records)
- Date/Time Selector
- Drop-down List
- Data Grid
- Information Box
- Label
- Link Label
- Listbox
- Number spinner
- Object Listbox
- Paragraph
- Radio Button
- Section Break
- Single Line Text Entry Box
- Sub Title
- Title
- Tree
- Form Layout Panel
- Group Box
- Layout Panel
- Tab Control
- Table Layout Panel
- Internet Browser
- Medias Explorer
- Media Player
- Object Explorer
- Search Control
- GIS Navigator Bar
- Open Layers Map
- Alert State Viewer
- Control Room Drop Zone
- Device Icon
- Drop Zone
- Icon

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
• Image
• KeyMap Selector
• Object Selector
• Perimeter
The GUI Designer shall include the following controls to design Process Guidance:
• Process Guidance Panel
• Confirm Task
• Yes/No Task
The PSIM Solution shall support a User Interface Control Development Kit that can be used to develop additional user interface components for the User interface Designer.

2.5.31 LOCALISATION

The PSIM Solution shall be available in US English for all configuration interfaces
The PSIM Solution shall be available in US English, Spanish and Arabic for all built-in operator screens
It shall be possible to translate all configurable display content
It shall be possible for multiple users to login using different languages
It shall be possible for the user to select language on the Login screen
The PSIM solution shall be capable of displaying operator user interfaces in the operator’s native language.

2.5.32 ADMINISTRATION INTERFACE

The PSIM system must have a powerful and friendly administration interface that includes wizards and summaries to help system administration for power users.
The administration interface must be configurable but must include the ability to add users, manage groups and schedules, roles and permissions, device status and summary, mappings and associations for cameras and alarms, site information and contacts.
An out-of-the box Administration Interface shall be available as a feature as part of the Windows Client
It shall be possible to restrict access to the Administration Interface to specific Users and/or Groups
The Administration Interface shall provide functionality to manage Users
The Administration Interface shall provide functionality to manage User Groups
The Administration Interface shall provide functionality to manage Contacts
The Administration Interface shall provide functionality to manage Contact Groups
The Administration Interface shall provide functionality to view the current state of connected devices
The Administration Interface shall provide functionality to generate reports on the state of devices
The Administration Interface shall provide a Health Check functionality displaying the integrity of the solution data and loaded device drivers

2.5.33 CONFIGURATION INTERFACE

The configuration interface shall be available (subject to user permissions) through the client application
It shall be possible to set breakpoints in workflows and step through these.
The System Configuration screen shall expose all properties available on objects under the control of the PSIM allowing an administrator to have one consolidated platform for configuring all aspects of the security integration process and management of devices.
It shall be possible to create a Trigger and a Workflow, matching variables for the event data and map all event data to variables in the Workflow through a simple command in the configuration interface
2.5.34 SECURITY POLICIES

The PSIM Solution shall include functionality to configure the following Client Policies:

- Acceptable Use Message: A message to be shown before users log on
- Account Lockout: Settings for when a user should be locked out and lockout time
- Allow multiple logons: Whether the same user account can be used to login on multiple clients at the same time
- Client Connection
- Do not display last user: Whether to display the last user name in the login box

The PSIM Solution shall include functionality to configure the following User Policies for specific Users and/or User Groups for a specific Folder/Location:

- Account Expiration Notification: The number of days before expiration that a notification is raised
- Add Clients: Gives permission to add clients to the folder
- Access to Admin Interface: Specifies who has access to the Administration interface
- Auto log off: Auto log off users when their associated Schedule goes out of scope
- Can exit Control Room Client: Whether users can exit the client application
- Message for users logging on: A message to be shown before users log on
- Can manage users and groups
- PTZ Lease: Specifies the PTZ Lease priority order for different users/groups
- Password Settings
- Access to Response Plan Designer
- Require String Password
- Access to System Configuration
- Video Export Administrator
- Video Export Deferrers
- Video Export Users

It shall be possible to change the following password settings:

- Enable complexity check
- Maximum Password Age
- Minimum Password Length
- Password History (the number of previous passwords to keep in memory)

2.5.35 WEB

The PSIM Solution shall include a Web Application Module

The Web Client shall Require Users to Login
The Web Client must be Capable of Viewing any Video from any Sub-System Integrated to the PSIM
The Web Application shall include Video Display Functionality allowing the User to:

- View camera feeds
- Access Recorded Video

It shall be possible to View Maps in the Web Client;
It shall be possible to Manage Alarms – View, Add, Comment and Close in the Web Client.
The PSIM solution shall be able to “Load Balance” Web Streaming Servers, allowing Video to be Transcoded and Scaled Upwards according to the number of Remote Users needing Access to Web Based Video.
It shall be possible to Allocate Streaming Servers to Specific VMS Sub-Systems.

2.5.36 APP FOR TABLETS AND CELL PHONES

The PSIM Solution shall include an App for Tablets and Cell Phones;
The App shall Require Users to Login;
The App must be Capable of Viewing any Video from any Sub-System Integrated to the PSIM;
The App shall include Video Display Functionality allowing the User to:
• View Camera Feeds;
• Access Recorded Video.
It shall be possible to View Maps in the App;
It shall be possible to Manage Alarms – View, Add, Comment and Close in the App;
The PSIM solution shall be able to “Load Balance” Web Streaming Servers, allowing Video to be Transcoded and Scaled Upwards according to the number of Remote Users needing Access to Web Based Video.
It shall be possible to Allocate Streaming Servers to Specific VMS Sub-Systems.
The App shall be available for at least:
• The latest iOS (Apple);
• The latest Android OS.

2.5.37 PROCESS GUIDANCE

The PSIM solution shall include visual Process Guidance components that can be linked to workflows.
A Process Guidance shall include any number of steps.
It shall be possible to configure a step so that the operator has to confirm an action or answer Yes or No to a question.
It shall be possible to park process guidance from the user interface.
Changes to process guidance shall become live when saved without any requirement for restarting the software or upgrading the software.
It shall be possible to use Graphical User Interface components as part of the Process Guidance.

2.5.38 TECHNOLOGY PLATFORM

The PSIM Solution shall be built using Microsoft technologies and on the .Net Framework 4.5 or later.
The server software shall be able to run on both multiple and single processor computers. Where a multiple processor system is used the workflow engine shall be able to make optimal use of that configuration.

2.5.39 SYSTEM INFRASTRUCTURE

The PSIM Solution shall use Microsoft SQL Server 2012 or later for its data store.

2.5.40 OPERATING SYSTEM REQUIREMENTS

The PSIM Solution components shall be able to run on the following operating systems:
• Core Service: Microsoft Windows Server 2012 or later
• Connection Manager: Microsoft Windows Server 2012 or later
• Rules Engine: Microsoft Windows Server 2012 or later
• Event Service: Microsoft Windows Server 2012 or later
• Notification Service: Microsoft Windows Server 2012 or later
• Alarm Types Service: Microsoft Windows Server 2012 or later
• Video Export Service: Microsoft Windows Server 2012 or later, Microsoft Windows 7 (64 bit), Microsoft Windows 8.1 (64bit) or later
• Windows Client: Microsoft Windows 7 (64 bit), Microsoft Windows 8.1 (64bit) or later

2.5.41 SOFTWARE LICENSING REQUIREMENTS
Software shall be licensed and permit growth over time. Software Assurance (PSM Maintenance) should be an integral of OPEX Costs to ensure that the PSIM solution is constantly managed and supported by the manufacturer. Sub system integrations such as ANPR shall be licensed via the master module [i.e. CCTV (VMS), Access Control (SMS), Intruder Detection (IDMS) and IP Intercoms (IP PBX)] Software shall be licensed based on the following:

- Number of devices
- Number of thick clients
- Number of thin clients
- Number of servers
- Total number of connected physical security devices
- Functionality, by module

The following master modules shall be licensable:

- CCTV / Video Management System (VMS)
- Access Control / Security Management System (SMS)
- Intruder Alarm / Intruder Detection Management System (IDMS)
- IP Intercoms (IP PBX)
- GIS Mapping
- AutoCAD

2.5.42 EXECUTION

The solution shall be built and Factory Acceptance Tested (FAT) by the solutions provider in the solutions providers’ configuration environment before it’s deployed on site. The solution can be built and Site Acceptance Tested (SAT) by the solutions provider in the solutions providers configuration environment before it’s deployed into Production. Deployment on site shall first be in a staging environment and promoted to production following successful User Acceptance Testing (UAT). Professional Services from the Manufacturer shall be provided to support the end user and partner in the deployment of the system. The solutions provider shall follow the documentation provided by the manufacturer.

2.5.43 FUNCTIONAL CAPABILITIES

The following section contains additional functionality that is included within the proposed PSIM system, but requires professional services to modify through system configuration, the ability to use these features.

2.5.43.1 GENERAL

There shall be available a set of Functional Capability modules that can be easily added to the PSIM solution. It shall be possible to add these additional modules at run-time. There shall be a well-documented process for adding pre-configured modules. It shall not be required to upgrade the core software version in order to add a new module.

2.5.43.2 GENERIC WEB PAGE VIEWER

The Web Page Viewer shall support displaying a specified web page from a workflow. The Web Page Viewer shall display the title of the displayed page passed in as a parameter form the workflow. The Web Page Viewer shall be capable of displaying the specified page on any logged in client workstation.
2.5.43.3 REPORTING

The Reporting module shall include a set of report templates for Microsoft SQL Server Reporting Services (SSRS)
The module shall use workflow functionality to generate reports through SSRS
The module shall include a user interface for generating each included report
The module shall include a Report Manager user interface, providing functionality for adding more reports
The module shall include a Report Viewer user interface
The module shall include three standard reports:
  • Alarm Counts
  • Alarm Details
  • Alarm Summary

2.5.43.4 ESCALATION

The module shall include functionality that can be called from process guidance in order to Escalate an alarm
When an alarm is escalated the process guidance shall be parked and closed for the handling operator
Then an alarm is escalated it shall appear in the alarm stack of operators assigned to handling escalated alarms
An Alarm Stack View shall be available that shows escalated alarms and can be provided to specified user groups

2.5.43.5 ALARM ACTIVITIES

There shall be a module that can display Alarm Activity linked to a specified alarm
The module shall include a user interface displaying the activity linked to the alarm
The Alarm Activity user interface shall show for each activity:
  • The Date and Time of the activity
  • The Operator
  • A description for the activity
  • The type of activity
It shall be possible to display the Alarm Activity user interface when handling an alarm
2.5.43.6  ALARM EVENTS

There shall be a module which can be used to display events linked to a specific alarm while handling the alarm.

The user interface shall display for each event:
- The Date and Time the event was received
- A description of the event
- The Alarm Point associated with the event
- The Location of the event

2.5.43.7  ALARM POINT SUPPRESSION

There shall be a module which can be used to suppress an alarm point.

When an alarm point has been suppressed, no alarm shall be generated for events received from the alarm point.

The module shall include a feature that we used from workflows to suppress an alarm point.

The module shall include a user interface that provides functionality for viewing and unsuppressing Alarm Points.

For each suppressed Alarm Point, it shall be possible to see:
- The user that suppressed the alarm point
- The time the Alarm Point was suppressed
- The number of events received since the Alarm Point was suppressed

For each event from a suppressed alarm point it shall be possible to see:
- The Date and Time the event was received
- The description of the event

2.5.43.8  DOOR OPTIONS

There shall be a module that provides a User Interface for performing common actions on a door.

The User Interface shall provide buttons that can be used to:
- Unlock a door
- Lock a door
- Provide Momentary Access for a specified time
- Block access to for badge holders for the door

2.5.43.9  PROCESS GUIDANCE

There shall be a preconfigured process guidance template that can be used when creating new process guidance.

2.5.43.10  ALARM RESOLUTION FORM

There shall be a pre-configure Alarm Resolution Form that can be shown to the operator when alarm handling is completed.

The Alarm Resolution Form shall include the following pre-populated fields:
- Alarm ID
- Alarm Priority
- Alarm Type Name
- Alarm Location
- Date/Time of alarm
- Top Location

The Alarm resolution form shall list all activities associated with the alarm and for each activity display:
- The Date and Time of the activity
The Alarm Resolution Form shall allow the operator to add additional comments to the alarm The Alarm resolution Form shall require the operator to select an Alarm Resolution Type It shall be possible to display the user interface for generating an Alarm Details report by selecting an option on the Alarm Resolution form before resolving the alarm

2.5.43.11 ALARM HISTORY

There shall be a Module for Display of Alarm History; The Module shall include a User Interface where the User can List Historical Alarms. It shall be Possible to Filter Alarms by:
- A Date and Time Range;
- A Number of Hours before the Current Time.
For Each Historical Alarm it shall be Possible to See:
- The Alarm ID;
- The Date and Time the Alarm was Created;
- A Description of the Alarm;
- The Resolving User;
- The Resolution Type Selected;
- The Date and Time the Alarm was Resolved.

2.5.43.12 NEAREST CAMERA MAPPINGS

There shall be a Module Providing Functionality to Associate Cameras to Alarm Points so that when an Alarm is Handled, the Specified Cameras can be Automatically Shown to the User; There shall be a User Interface where the User can Create New Associations between an Alarm Point and a Set of Cameras; The User Interface shall allow the User to Delete the Alarm Point Associations; When an Alarm is Handled, any Associated Cameras shall be Shown.

2.5.43.13 OBSERVED ALARM

There shall be a Module that allows the User to Manually Create Alarms in the System; The User Interface shall allow the User to Specify:
- The Alarm Type;
- The Location of the Alarm;
- Comments for the Alarm. It shall be possible to schedule an alarm so that it is generated at a specific Date and Time. This is so that for instance a Guard Round alarm can be generated and handled at a specific time of the day, implementing a process for performing a set of Guard Round tasks; There shall be a User Interface to View and Cancel Scheduled Alarms.

2.6 INTEGRATION OF SUB-SYSTEMS INTO THE PSIM SOFTWARE

The following subsystems shall be incorporated into and shall form part of the integrated security system:

CCTV / Video Management System (VMS);
Access Control / Security Management System (SMS);
Intruder Alarm / Intruder Detection Management System (IDMS);
IP Intercoms (IP PBX);

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
Installation Requirements and Rules;
UPS Monitoring;
Graphical Display;
Event Logging System.

Location, Access and Access Levels to Integrated Security System

The Integrated Control System Operator’s Monitors will be situated in the Security Control Room.

The security control room operators will report for duty and will only be granted usage and Control of the Security Control System, once he/she has logged in his Personalized Control System Pin Password on the Operator’s Key Board. Alternatively he/she can be given Access through a Card or Biometric Reader that is installed on the Control Room Workstation for this purpose.

The level of Operator’s Control of the Security System will be determined by the Head of Security of the campus and will be set out in the Security Operating Procedure (SOP).

The following levels of control room access are envisaged:

2.6.1 SYSTEM INTEGRATOR

This is the highest level of access that will provide the user full usage of the entire security control system as well as also provide and include full manipulation of software.

2.6.2 SUPERVISOR

This level of access will provide the operator full usage of the system inclusive of the opening of doors, the registering of new control room operator staff, access into the event logging system, manipulation of the levels of access given to existing control room staff and the full usage of the review of any recorded material and full usage of the CCTV system, Access Control System, Intruder Detection System and IP Intercom System.

2.6.3 SECURITY SHIFT SUPERVISOR

At this level of access the operator will have full access to the event logging system and will provide the operator the full use of the CCTV system, Access Control System, Intruder Detection System and IP Intercom System inclusive of the Review of all Recorded Cameras.

This operator will however not be able to add, delete or modify any of the control room staff on the security control system. He will be able to accept any alarm condition.

2.6.4 CONTROL ROOM OPERATOR

This level of Control Room Operator will be able to view and control the CCTV system, Access Control System, Intruder Detection System and IP Intercom System and provide monitoring capabilities for the balance of the icons.

The operator will be able to Accept Alarm Conditions from all included Sub-Systems up to the level of access that will be provided to him during his work shift by the Supervisor.
2.6.5 CCTV SYSTEM / VIDEO MANAGEMENT SYSTEM (VMS)

The CCTV System shall be fully integrated to the PSIM.

The CCTV Matrix(s) shall be integrated with the PSIM via a high level Interface (HLI) at each workstation or server.

The full functionality of the system shall be integrated with the PSIM to provide enhanced features including but not limited to:

- Camera to Monitor Commands;
- Sequence to Monitor Commands;
- Sequence Programming Commands;
- Pan, Tilt, Zoom commands;
- PTZ Pre-set Select Commands;
- PTZ Pre-set Save Commands;
- Monitor Blanking Commands;
- Black Screen Technology.

The CCTV system shall consist of a modular and distributed matrix system, which shall provide the switching capability of video signals from cameras installed throughout the facility.

The High Level Interface (HLI) shall provide the logical connections with other security sub-systems such as the locking, Intercom and Digital Video recording systems.

Integration of the CCTV system with the PSIM via potential free contacts shall not be accepted.

Access Control / Security Management System (SMS)

The Access Control / Security Management System (SMS) shall be integrated with the PSIM via a high level Interface (HLI).

The full functionality of the Access Control System shall be integrated with the PSIM to provide enhanced features including but not limited to:

- Door Lock;
- Door Unlock;
- Door Inhibit;
- Door Lockdown;
- Door Lockdown Time Pre-set;
- Door Status Monitoring;
- Door Alarm Annunciation;
- Door Auto-Close;
- Hardware Fault Diagnostics including Battery Status of Wireless Door Locks.

2.6.6 INTRUSION DETECTION SYSTEM (IDMS)

The Intrusion Detection System shall be Integrated with the PSIM to monitor specific hardwired and wireless alarm I/O points within the campus via a High Level Interfaces (HLI).

The full functionality of the intrusion detection sub-system shall be integrated with the PSIM to provide enhanced features including but not limited to:

- DPS Monitored Door Alarms;
- Panic / Duress Alarms;
- Passive Infrared Sensors;
2.6.7 LOG-ON SYSTEM

The Log-On System shall control the Log-On status of all Operator Workstations, which shall be achieved via Biometric Fingerprint Readers installed at each Operator Workstation.

2.6.8 IP INTERCOM SYSTEM (IP PBX)

The IP Intercom System hardware shall be integrated with the PSIM via a High Level Interface (HLI).

The full functionality of the system shall be integrated with the PSIM to provide enhanced features including but not limited to:

- Station Call-In;
- Station Fault Analysis;
- Call In Divert;
- Call Answer;
- Call Cancel;
- Call-In Queuing;
- Tamper Alarm monitoring;
- Threshold Monitoring (Disturbance detection);
- Individual Station Speaker and Microphone sensitivity adjustment;

The IP Intercom System shall Enable the Selection of any Individual or Group of Intercom Stations by any Operator Workstation within the Campus.

2.6.9 CENTRALISED UPS SYSTEM

The full dual redundant centralized UPS’ shall be fully integrated with the Security Management System by means of a High Level Interface (HLI), to provide operators and technicians with detailed status and alarm conditions regarding the UPS systems.

Due to the Centralized configuration, the following detailed diagnostic information is required, and shall be presented to the operator via a drop down menu option within the PSIM:

- Battery Data:
  - Battery Status;
  - Time Remaining in minutes;
  - Remaining Charge in %;
  - Battery Voltage;
  - Battery Temperature in °C.
- AC Input Data:
  - Voltage per phase;
  - Power per phase.
- AC Output Data:
  - Voltage per phase;
  - Power per phase;
  - Load % per phase.
UPS Alarm Conditions:
- Battery Failure;
- On Battery Power;
- Low Battery;
- Depleted Battery;
- Over Temperature;
- Output Overload;
- Bypass Active;
- Charger Failure;
- Fan Failure;
- Fuse Failure;
- Communications Failure;
- Shutdown Pending;
- Shutdown Imminent.

All alarm conditions shall be presented to the operator within the Fault queue as described in Section 2.14.2.11 of the specification.

2.6.10 SOFTWARE CONFIGURATION

The entire un-coded software (this is the software that will be configured by the contractor to integrate the various sub-systems during the contract, to comply with the requirements as detailed in this specification) shall be provided at the end of the contract to enable the staff of the CLIENT to fully re-load the entire configured programming package onto their server in the case of computer failure.

Training to all the security staff members of the CLIENT shall further be provided by the successful tenderer at the end of the contract, in the full use of the installed sub-systems and all relevant software packages, to enable them to fully understand, configure and operate the final installed product. Sufficient training Manuals will be prepared and provided to the number of staff members to be trained, by the tenderer, and the organizing of the training will be the responsibility of the tenderer and must be arranged it between themselves and the client.

2.6.11 GRAPHICAL DISPLAY

The Integrated System GUI shall support a minimum of 200 colour maps for the purpose of displaying the location and real time status of any integrated system input or output.

Graphical maps to be included within the initial configuration are to show in detail the following areas:

- Site plan showing all buildings and locations of all alarm points and operator workstations.
- All buildings devices/status/alarms and the like.
- All building tamper, communications, power and the like.
- Other maps as required to clearly display all alarm input within buildings.

Graphical Maps shall comply with the following:

- Each site map shall be provided with a site plan key, which shall be common to all maps and situated in the same position. The key shall provide a means for the operator to quickly navigate through the entire facility without the need to use standard navigation buttons or the main site map.
- All device location and statuses shall be detailed on each map and coloured accordingly for ease of recognition of both the device type and real time status.
- Text messaging identifying the device type, designation and alarm status shall be available in a “mouse over” or “icon” pop-up screen structure to minimize text on individual maps.
All text descriptors shall be approved by the Engineer prior to final acceptance. Liaise all requirements through the Engineer when programming these maps and other alarm/response descriptions.

Function key descriptions shall also be displayed as mouse over or pop-up screen hints. Graphical map displays shall be of high resolution to enable accurate images to be represented.

The system shall allow maps to be linked by means of navigation buttons to allow operators to "zoom" in or out to display either additional detail or an overall map. Point status and locations shall be clearly displayed using colour-coded icons. All icons shall display real time status of each point with continuous updates being provided to any dynamic screen display. Updates shall occur every 1 second or less.

2.6.12 CURRENT ALARM WINDOW

The system shall provide an efficient and reliable alarm handling procedure and shall include both audio and visual annunciation, logging to the database and recording of the history file the device description, point description, location, time and date the alarm occurred. The system software shall have the ability to route only selected alarms to specific operator workstations, allowing different locations or applications to be segregated on a building or system basis.

All systems activity shall be presented to ensure proper actions have been taken and that no alarm is left unattended for any lengthy period. Alarms, which have been acknowledged, and not cleared/reset shall be clearly distinguishable.

Upon occurrence of an alarm(s) a user configurable audible tone shall sound at the operator workstation(s) and display an indication of the incoming alarm together with its priority. If there are additional alarms to acknowledge the operator’s station shall continue to sound the appropriate alarm tone, display the number of alarms waiting and identify the highest priority alarm. The first alarm displayed shall be the highest priority alarm followed by the next highest priority alarm, etc.

All alarms are required to be separately acknowledged by the operator, by means of the mouse provided to acknowledge and reset each alarm separately. Each time new alarms are created the system shall restack the alarms so the operator sees them in order of priority.

The system shall also have an alarm/event status display available to the operator at all times on the operator's station. The display shall be a real-time dynamic display of alarms in the active state, or system component failures.

An audit trail shall be used to log the actions taken by all system operators in response to an alarm. The audit trail shall note:

- When the Alarm was Activated;
- When the Alarm was Acknowledged;
- Who Acknowledged the Alarm;
- When the Alarm was Restored.

The system shall record every user command, acknowledgment and log every operator login. These transactions shall be routed to the history database.

Any alarm point which has been suppressed/inhibited by the operator shall on expiry of the time zone, or when unsuppressed by the operator, generate an alarm if the alarm point is in the "active" state. The report to the operator terminal shall be the same as described above.
Each alarm point shall have the facility for a description of the alarm occurring. A comprehensive outline for operator instructions, detailing all response actions shall be provided for all alarms.

2.6.13 SYSTEM CONFIGURATION

The Operator workstations shall serve as the graphic based operator interfaces between the security officers and the integrated security systems as specified herein. All operator functions shall be controlled by means of a mouse, and shall require the minimum movement and actions in order to complete a required task. Alarm processing, alarm logging, alarm response data entry, graphical and text based user interface, data entry, and other system management functions shall be performed by the GUI operator workstations. The operator workstations shall be located in the Central Control Room.

The GUI shall be fully programmable to allow:
- Response instructions to be displayed for all alarms types;
- Use dynamic (real time) graphics to display device status;
- Initiate operator commands via system tailored icons;
- Display building layouts in a graphical representation.
- Easy to follow menus with single key select options, to assist in the daily routine operations of each facility;
- Allocate alarm priorities;
- Set alarm response properties;
- Set lock/unlock and access/secure operating schedules;
- Generate User defined reports.

The contractor shall allow adequate time to liaise with the Engineer in order to detail any user specific requirements necessary for the operation of each building, system, alarm type, and alarm response configuration within the system. This shall include the configuration of maps, report formats, access schedules, alarm response instructions and the like, to suit each operator workstation.

The system shall be modular in design to allow for future system expansion (i.e. in excess of 200 % of specified capacity) with minimum cost and disruption to the existing operational system.

Tenderers are to specify the systems total capacity for future expansions. Such upgrades shall not render a redundancy in field hardware, the Central Processing Units or any major component of software, firmware or operating systems.

2.6.14 SYSTEM PERFORMANCE

2.6.14.1 CENTRAL OPERATOR WORKSTATIONS

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation shall be no greater than one second (1 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (color) shall be no greater than one second (1 sec).

The interaction delay between recalling any floor plan at any given operator workstation shall be no greater than one quarter of one second (0.25) second.

2.6.14.2 LOCAL OPERATOR WORKSTATIONS (WHERE APPLICABLE)

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation shall be no greater than one half of one second (0.5 sec).
The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (color) shall be no greater than one half of one second (0.5 sec).

2.7 SECURITY MANAGEMENT FUNCTIONS

2.7.1 CONFIGURATION

The PSIM shall consist of a multiple screen representation of the entire facility, which shall contain all of the necessary icons to control all security sub system equipment and devices situated throughout the prison. All icons shall be activated with the use of a mouse. All icons and status indicators shall be a minimum of 5mm in diameter. All symbols shall provide status by colour and/or associated text. All symbols shall be to the approval of both the Engineer as well as the representatives of PDW and DCS.

2.7.2 GLOBAL FUNCTION OPERATIONS

Global function icons shall be located at the bottom of each graphic screen in the form of a footer window, which shall be common to all area maps. These icons, if active, shall control the global functions for the entire facility.

2.7.3 SYSTEM CONTROL

Activating this icon shall cause the system to switch to the system control screen. The System Control screen shall provide a complete system diagnostic window for all sub-system components and communication systems within the entire facility.

The diagnostic information shall include but not be limited to the following:

- UPS System:
  - Load on Bypass;
  - Load Not Protected;
  - Mains Failure;
  - Battery Fault;
  - Battery Low;
  - Surge Arrestor Failure;

- Control Hardware Status (Per Zone):
  - TCP/IP communication Failure;
  - Control Network communication Failure;
  - Device Network communication Failure;
  - I/O Device Failure;
  - Communication Redundancy Integrity;
  - CCTV Matrix communication Alarm;
  - Door position switch violation alarm per DPS;
  - Controlled door security violation alarm per door;
  - Fire door security violation alarm per door;
  - Panic Button activated alarm per Panic Button;
  - Intercom Call In Failure per Intercom;
  - Operator Log On Violation.

Where applicable all alarm conditions shall allow for operator acknowledgement and automatic selection of the alarmed zone layout screen.

2.7.4 SITE PLAN
The site plan shall consist of an interactive miniature layout of the entire facility, and shall be situated on the bottom Right hand side of each operator screen.

The site plan shall provide the operator with a quick method to access an individual area to monitor and / or control.

**The site plan shall also indicate critical operational information to the operator, which shall include but not be limited to the following:**

- Doors Unsecured
- Local Control Room Logon Status
- Local Control Room Call In
- Local Control Room Communication Alarm

## 2.7.5 FAULT QUEUE

The PSIM footer window shall contain a Fault queue facility into which all security sub-system or control system faults are entered in order of priority.

Upon receipt of any security sub-system or control system fault, the relevant fault detail including the control area, equipment designation and the specific location of the fault shall displayed as a pop-up screen on the Graphical display. Upon acceptance of this fault by the control room operator by selection of the “Alarm Accept” icon the fault shall be entered into the Fault queue. By selecting this icon the control room operator accepts full responsibility for acceptance and reporting of the alarm, as this event is logged into the event logging system.

The Fault queue is intended to provide a quick reference to the system operator of current alarms.

**Faults may be dealt with in the following ways:**

By right clicking on a specific fault in the queue, the operator shall be presented with an “Acknowledge” option again. Clicking on the Acknowledge option shall enter the acknowledgement into the event recording system again. The fault shall remain in the fault queue until such time that the fault is cleared. Only then will the fault automatically remove itself from the fault queue.

By double clicking on a specific fault in the queue, the appropriate area map shall be displayed with the faulty equipment control icon clearly visible. The equipment icon shall display the fault detail in a mouse-over or "hint" fashion. Right clicking on relevant equipment icon shall present the operator with an “Acknowledge” option again. Clicking on the Acknowledge option shall enter the acknowledgement into the event recording system again. The fault shall remain in the fault queue until such time that the fault is cleared. Only then will the fault automatically remove itself from the fault queue.

Local operator workstations shall display alarms and faults related to the immediate area of control only. Central operator workstations shall display all current alarms within the entire campus.

## 2.7.6 SYNCHRONIZED CLOCK SYSTEM

All operator workstations footer windows shall contain a synchronized digital clock, which indicates the Date and Time in 24 Hour mode. The accuracy of the synchronised digital clock system shall be within ± one (1) minute within a thirty (30) day period, and shall be synchronised with the PSIM Server within the Central Control Room each hour on the hour.

## 2.7.7 OPERATOR LOGON DETAILS
The PSIM footer window shall contain the detail of the currently logged on operator including full name and authorized user level.

2.7.8 BLACK SCREEN TECHNOLOGY

The PSIM shall provide integrated Black screen technology, which shall enable the automatic selection of relevant Cameras to allocated Monitors in the case of a Detection alarm. The PSIM through its high level interface to the sub-system hardware shall make logical selections of pre-set camera images to the alarm zone. The system shall allow for three simultaneous alarm conditions with cameras pre-set to include the full zone in each case. Once an alarm has been activated and the camera pre-set to that zone, the control room operator shall be able to zoom in on the specific fault thus providing valuable recorded material for later use by the authorities. Once an alarm is triggered, the relevant zone PTZ / Camera image shall be switched to the monitor. The technology is required to ensure that all alarm conditions are brought to the attention of the Central Control room operators immediately, and to present them with the necessary information to respond to the event. The PTZ pre-set position monitor allows the operator to immediately view the alarm zone, and to follow the offender via the PTZ control functions.
3 SECURITY MANAGEMENT SYSTEM (SMS)

3.1 GENERAL

The Security Management Software System shall be capable of including at least the following components:

- Access Control Server(s);
- Operator Workstation(s);
- IP Converter(s);
- Door Controllers;
- Card Readers (whether they are Proximity, Magnetic Stripe or Barcode or any combination of the above technologies);
- Semi-Online Access Control [Sallis (by SALTO) Wireless Locks].
- Biometric Readers.
- Breakglass Units.
- Key Overrides.
- Magnetic Locks.
- System Software.
- Front Desk and Card Printing Software.

The following diagram explains the relationship of these system components:

![Diagram](image-url)
3.2 SOFTWARE

Minimum Software Requirements:

The Security Management System (SMS) software shall be designed specifically for this type of environment and shall have a proven track record in the industry. The software shall be an Off-the-shelf package available through a distributor network. The off-the-shelf software shall be programmed and tailored to the specified functions and features described herein and as indicated on the accompanying drawings.

The software shall convey an accurate floor plan of all areas that require display. The software shall utilize the maximum resolution and colours of the Full HD Monitor to enhance and simplify the displayed control and status information. Fast orientation and ergonomics will be the goal of the graphic displays.

The software shall provide integrated Biometric (Fingerprint) log-on security functionality with security level protection for all Mouse driven operator workstations. The Biometric (Fingerprint) logon facility shall be capable of providing a one to many search algorithm to confirm operator credentials, without the need for entering user details or the swiping of a personal identification card. It must be noted that although this software may be an additional software package the same protocol of the two software packages is not negotiable.

There shall be a minimum of ninety nine (99) levels of access, and shall be expandable.

The software shall provide on-line utilities accessed through the Management workstation menu structure. These utilities shall provide the system supervisor with the ability to edit and update required data bases, system operating variable, report configuration and generation, alarm tags and point descriptions, etc. These utilities shall be protected by security levels and Biometric Access.

All software licenses shall be transferred to the Owner at completion of the project. This shall include but not be limited to all original installation disks, software manuals, equipment manuals, etc. All project specific applications software shall be transferred at the end of the contract period.

3.2.1 SYSTEM CONFIGURATION

The Interactive Security Management System (SMS) shall consist of a server and multiple Operator Workstations, situated in the local, central control rooms and any other location so required by the University.

The Operator workstations shall serve as the graphic based operator interfaces between the security officers and the campus’s locking controls system and other security subsystems as specified herein.

All operator functions shall be controlled by means of an optic mouse, and shall require the minimum movement and actions in order to complete a required task.

All security sub-system control functions shall be interlocked to ensure that functional procedures are adhered to.

Alarm processing, alarm logging, alarm response data entry, graphical and text based user interface, data entry, and other system management functions shall be performed by the SMS operator workstations connected to the data network. The operator workstations shall be located in the Central Control Room and other nominated locations.

The Security Management Servers shall reside on a Virtual Environment using Hypervisors and VMs.
The system shall be designed such that failure of any control module or operator workstation shall not functionally affect the operation of any other module, network, building or Operator workstation connected to the data network.

Similarly, should any area lose power or suffer a loss in communications due to a break in the communications cabling, all Distributed control modules installed in that area shall continue to operate with no loss of functionality.

The SMS shall be fully programmable to allow:

- Response instructions to be displayed for all alarms types.
- Use dynamic (real time) graphics to display device status.
- Initiate operator commands via system tailored icons.
- Display building layouts in a graphical representation.
- Easy to follow menus with single key select options with pop-up screens located on the display, to assist in the daily routine operations of each facility on campus.
- Allocate alarm priorities.
- Set Alarm response properties.
- Set lock/unlock and access/secure operating schedules.
- Generate User defined reports.

The tenderer shall allow adequate time to liaise with the Engineer and University representative in order to detail any user specific requirements necessary for the operation of each building, sub system, alarm type, and alarm response configuration within the system. This shall include the configuration of maps, report formats, access schedules, alarm response instructions and the like, to suit each operator workstation.

The system shall be modular in design to allow for future system expansion (i.e. in excess 200% of specified capacity) with minimum cost and disruption to the existing operational system.

Tenderers are to specify the systems total capacity for future expansions. Such upgrades shall not render a redundancy in field hardware, the Central Processing Units or any major component of software, firmware or operating systems.

The tenderer shall note that all programmed software done in order to integrate all the sub systems and all other software, being written or purchased shall be the property of the University after hand over.

All un-compiled software shall form part of the final documentation and shall be handed over in three fold to the University after commissioning of this installation.

### 3.2.2 SYSTEM PERFORMANCE

#### 3.2.2.1 CENTRAL OPERATOR WORKSTATIONS

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation, (i.e., the lock), shall be no greater than one second (1 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (colour) shall be no greater than one second (1 sec).

The interaction delay between recalling any floor plan at any given operator workstation shall be no greater than one quarter of one second (0.25) second.
3.2.2.2 LOCAL OPERATOR WORKSTATIONS (WHERE APPLICABLE)

The interaction delay between activating a control icon on any given operator workstation and the controlled point activation, (i.e., the lock), shall be no greater than one half of one second (0.5 sec).

The interaction delay between controlled point activation and any given operator workstation response either by activation of an audible alarm and/or the associate icon changing state (colour) shall be no greater than one half of one second (0.5 sec).

3.2.3 GENERAL REQUIREMENTS

The Access Control Server(s) and Operator Workstation(s) as well as the application software (herein referred to as the Security Management Software – SMS) shall be used to provide a total, Real Time, Access Control and Attendance management system using menus, function keys and icons coupled with dynamic graphic user interfaces.

The SMS shall upon a server or PC reboot due to an AC power failure or any other reason recover all functionality even if no operator logs in.

3.2.3.1 OPERATING SYSTEM AND COMPUTER HARDWARE PLATFORMS

It is an express requirement of this tender that the contractor shall offer an integrated (SMS) which is optimized to operate on any standard Intel® Pentium® Xeon® server employing Microsoft® Windows Server 2012 or later operating system.

The SMS software application shall be designed to utilize the latest features provided by the Windows graphical user interface (GUI). Software applications designed for DOS, 16-bit versions of Windows, or Windows 95/98 shall not be acceptable.

Furthermore, the contractor shall provide guarantees that all computer equipment (including expansion boards and peripherals) are compatible with the Microsoft® Windows Server 2012 or later Operating Systems.

3.2.3.2 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. Preference will also be given to products developed and manufactured in South Africa. In any 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.

3.2.3.3 SYSTEM INTEGRATION AND EXTENSIBILITY

3.2.3.3.1 SOFTWARE DEVELOPERS KIT (SDK)

The SMS shall support an SDK to allow for external third party applications like the PSIM to interact with it. It shall also provide for external event and alarm monitoring and control back into the application in an XML format.

API – There shall be available as an option, an Application Programming Interface to allow third party applications to manage Users and Credentials in the Security Management application, including add, edit, and delete functions.
XML – There shall be available as an option, an XML interface to allow for the Security Management application to receive commands in an XML format, as defined by the SDK, to perform commands like: List Alarms, Acknowledge Alarms, Unlock Doors, issue Command Sets, and others, and to provide command responses in an XML format.

The Vendor shall have available a Professional Services Group to assist and/or provide solutions using the SDK.

If a Software Development Kit is unavailable the software vendor shall do the necessary changes to the software for the CLIENT at no additional charge. If none of the above requirements can be met the Access Control System will not be considered.

3.2.3.3.2 DATABASE

The SMS shall employ the latest available open database technologies to provide a transparent interface to the system database. These database technologies shall allow the SMS 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 any common database management system, including Microsoft SQL Server.

3.2.3.3.3 ARCHITECTURE

The architecture of the SMS shall allow the modular implementation, commissioning and decommissioning of segments of the system to suit client requirements. The system shall be capable of consolidating Visitor, Employee/Student and card Reader transaction data from separate SMS servers 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 the entire access control installation.

3.2.3.3.3.1 GENERAL

The Security Management System (SMS) shall be written to be fully SOA compliant.

Service-Oriented Architecture (SOA) is a software solution intended to enable the enterprise to organize and marshal multiple processes.

With SOA, software applications no longer are massive bundles of functions and processes. Instead, applications are composed by assembling modular services.

A service is a single software function – such as: open door, call intercom, etc. It can be executed on demand by any system, without regard to its operating system, platform, programming language, or geographic location. Just as web pages load on any platform, web services work the same regardless of platform, provided they are built using universal standards.

Developers build composite applications by interconnecting, or “orchestrating,” services in a process flow. This flow can then, itself, be structured as a service. Developing such composite web services is often called Business Process Management. Standard SOA tools streamline the task of building service-orchestration models–similar to creating a flow chart.

A more useful nomenclature might be Service Orientation (or SO). There are actually a number of parallels with Object Orientation (or OO) and component-based development (CBD):
Like objects and components, services represent natural building blocks that allow us to organize capabilities in ways that are familiar to us; Similarly to objects and components, a service is a fundamental building block that:
- Combines information and behaviour;
- Hides the internal workings from outside intrusion;
- Presents a relatively simple interface to the rest of the organism.
Where objects use abstract data types and data abstraction, services can provide a similar level of adaptability through aspect or context orientation; Where objects and components can be organized in class or service hierarchies with inherited behaviour, services can be published and consumed singly or as hierarchies and or collaborations.

### 3.2.3.3.2 PRINCIPLES AND DEFINITIONS

**SOA** – The policies, practices, frameworks that enable application functionality to be provided and consumed as sets of services published at a granularity relevant to the service consumer. Services can be invoked, published and discovered, and are abstracted away from the implementation using a single, standards-based form of interface.

**Service**

A Service is a capability by which the need of the Service Consumer or Requestor is satisfied according to a contract; Separate the what from the how, who and where; Manage and govern through policies and contracts; Communicate using messages that share schema not technology; Are discoverable, at design and run-time.

### Core SOA Characteristics

1. **Loose Coupling**
   - Enabling rapid process integration & optimization

2. **Functional standardization**
   - Reuse to reduce cost and deliver consistency across different solutions

3. **Consumer (solution) flexibility**
   - Use alternative and or specialize services

4. **Resource virtualization**
   - Who, What and Where

**Usage decisions determined by Policy**

**Supplier flexibility**
- Use alternative and consolidated resources

### 3.2.3.3.3 SUMMARY
The goal for a SOA is a worldwide mesh of collaborating services, which are published and available for invocation on the Service Bus. Adopting SOA is essential to deliver the business agility and IT flexibility promised by Web Services.

These benefits are delivered not by just viewing service architecture from a technology perspective and the adoption of Web Service protocols, but require the creation of a Service Oriented Environment that is based on the following key principals:

- Service is the important concept. Web Services are the set of protocols by which Services can be published, discovered and used in a technology neutral, standard form;
- SOA is not just an architecture of services seen from a technology perspective, but the policies, practices, and frameworks by which we ensure the right services are provided and consumed;
- With SOA it is critical to implement processes that ensure that there are at least two different and separate processes—for provider and consumer;
- Rather than leaving developers to discover individual services and put them into context, the Business Service Bus is instead their starting point that guides them to a coherent set that has been assembled for their domain.

3.2.3.3.4 PROJECT SPECIFIC

All settings, interfaces, etc. shall be modifiable by the user and fully parameter driven;
Any service, configuration change, etc. shall be accessible and may not be more than 2 mouse clicks away;
All protocols and interfaces shall be interchangeable;
Interconnectivity must be transparent. All interfaces shall be defined in a user manual.

3.2.3.4 VENDOR AND INSTALLER CREDENTIALS

The software vendor shall preferably be accredited as a Microsoft Certified Solution Provider. At a minimum, the software vendor shall have at least five (5) years’ experience in the development of software applications for Microsoft Windows Server Operating Systems.

The tenderer shall be certified by the Access Control hardware and software vendor as an approved installer of the proposed SMS. 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 SMS. It shall be incumbent upon the tenderer to prove compliance with these requirements.

3.2.4 ACCESS CONTROL SOFTWARE

The SMS application software shall provide a graphical interface to the functionality provided by all Access Control hardware that forms part of the proposed system.

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

- System Administration and Maintenance;
- Customisation Manager;
- Enrolment Manager;
- Report Manager;
- SQL Manager;
- Task Scheduler;
- Configuration of Associated Hardware;
- Communications Interfaces:
  Serial (USB, RS232, RS422 & RS485) Modems etc.

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
TCP/IP.
Add or Remove Hardware;
Command Sets;
Workstation(s);
Administration of Employee/Students and Visitors;
Time Zones;
Holidays;
Badge and Graphics Designers and Card Printing Interface;
Management of Access Control for Individuals and Groups;
Credential Templates;
Door Groups;
Function Groups;
Student Groups;
Assigning Operator Permissions;
Operators;
Operator Groups;
System Operation;
Status Viewer;
Graphics;
Alarm Viewer;
Event Viewer;
Browser;
Video Explorer;
CCTV Camera Viewer.

Starting the main application for the SMS will automatically start all sub-applications and services. This implies that putting one application into the startup menu of Windows will start all parts of the SMS.

3.2.4.1 APPLICATION SETTINGS

Administrators shall be able to configure the SMS software by invoking a software configuration ("options") 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;
Behavior of key software modules;
Definition of Employee/Student Access Levels (to facilitate greater control of high security areas);
Backup Schedules and Location of Backup files;
Default Access Control Templates for Employee/Students and Visitors;
Labels of user-defined data fields in Employee/Student and Visitor Records;
Date and Time formats;
Video Capture pixel resolution, aspect ratio, file format and image quality.
Synchronization of System Time:
Set the PC or Server to use as the Global Clock as well as a backup PC or Server should the Global Clock not be available on the network at the time of synchronization.
Synchronization Times.
Daily;
Weekly;
Monthly;
Etc.
A do not synchronise at this time function.
3.2.4.2 OPERATOR ADMINISTRATION

The SMS shall employ Operator Groups to control the permissions of Individual Operators and Groups of Operators. Administrators shall be able to control access to the system's functionality by creating Operator Groups, defining the permissions of those Operator 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 Operator and the period for which he/she will remain a valid Operator.

The software shall allow Administrators to control which Employee/Students, Access Control Groups, Readers and Zones a specific Operator Group is authorized to manage.

**Systems that allow Administrators to configure permissions separately for each Operator will be the preferred type, but as a minimum the following levels will be required:**

- Operator - Type 1  e.g. Alarms Monitoring;
- Operator - Type 2  e.g. Sensitive Areas Monitoring;
- Supervisor;
- Site Administrator;
- Systems Administrator;
- Report Printer.

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

Users shall be required to log on to the system by typing in a username and password, presenting their access cards, or by presenting a biometric print at a card Reader or biometric Reader which has been designated as the log-on Reader for a specific workstation (These Readers shall be attached directly to the workstation via USB or serial interface).

3.2.4.2.1 LANGUAGE SUPPORT

The proposed SMS software application shall have the capability to present its interface in the language of a user's choice. It shall be possible to select the user interface language for each authorized operator. When a user logs on to the system, the user interface shall be presented in the language specified in that user's preference settings.

At a minimum, the user interface shall be available in English. The software vendor shall provide all the tools necessary to translate the user interface into any language supported by the Microsoft® Windows® 7 or later and, Windows® Server 2012 or later operating systems.

3.2.4.3 EMPLOYEE/STUDENT MANAGEMENT

An Employee/Student management module shall provide an interface allowing users to manage all data pertaining to Employee/Students.

3.2.4.3.1 EMPLOYEE/STUDENT CONTROL

Administrators shall be able to assign control of any Employee/Student Group to any user Group. A user's ability to control cardholder records and Access Control permissions shall be controlled by permissions set for the user Group(s) of which that user is a member. Duly authorized operators shall be able to assign zone and Reader access permissions simultaneously to the members of an entire Employee/Student Group.
3.2.4.3.2 EMPLOYEE/STUDENT DATA

Data accessible from the Employee/Student management module shall include the following types of information:

- Personal Details (e.g. title, first names, surname, Employee/Student number, ID number, gender);
- ID cards and/or Personal Identification Numbers (PINs) assigned to the Employee/Student;
- Card/PIN validity, time and attendance logging options, access levels;
- Photographs;
- Contact Details;
- Company and Department to which Employee/Student is assigned;
- Zones to which Employee/Student has access;
- Readers at which Employee/Student is allowed access;
- Groups to which Employee/Student belongs or Multiple Groups;
- Schedules specifying the periods during which an Employee/Student will be granted access at a specific zone or Reader;

In addition to these standard data fields, the Employee/Student record shall provide at least five (5) additional fields for the entry of user-definable data.

3.2.4.3.3 CARDHOLDER MANAGEMENT

The SMS shall provide fully integrated functionality for the recording of cardholder information and the issuing of cards.

3.2.4.3.4 CARD / PERMISSIONS ASSIGNMENT

Operators shall be able to assign an ID card from within the Employee/Student Management Module by activating a take-on Reader connected to the workstation. It shall be possible to assign multiple ID cards to an Employee/Student and to assign an alias name to each additional card. The system shall be able to address additional cards by whatever alias names have been assigned to them.

A duly authorized operator shall be able to issue a temporary card to an Employee/Student. When a temporary card is issued, it shall inherit the Access Control permissions that have been defined for the Employee/Student's permanent card. The issuing of a temporary card will cause an Employee/Student's permanent card to be disabled for as long as the temporary card remains valid. It shall be possible to specify that a temporary card is valid only for the day on which it is issued. The operator shall also be able to specify that a card be deposited in a drop box when the cardholder exits at a specific Reader.

The system shall automatically consolidate time and attendance data for all cards issued to an Employee/Student.

It shall be possible to specify the activation and expiration times of a card unambiguously in hours, minutes and seconds on any day of any month of any year in the future (e.g. 2005/12/31, 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.

3.2.4.4 VISITOR MANAGEMENT

A Visitor management module shall provide an interface allowing users to manage all data pertaining to Visitors.
3.2.4.1 VISITOR DATA

Data accessible from the Visitor Management Module shall include the following types of information:

- Personal Details (e.g. title, first names, surname, ID number, gender);
- ID cards assigned to the Visitor;
- Date and time when the validity of a card commences, and period for which card will remain valid. The following options shall be available as a minimum:
  - Any number of hours;
  - 1 day or any number of days;
  - 1 week or any number of weeks;
  - 1 month or any number of months;
  - 1 year;
  - Indefinite.
- Photograph of Visitor;
- Contact Details;
- Company and Department which the Visitor is visiting;
- In addition to these standard data fields, the Visitor record shall provide at least five (5) additional fields for the entry of user-definable data.

3.2.4.2 CARD / PERMISSIONS ASSIGNMENT

Operators shall be able to assign an ID card from within the Visitor management module by activating a take-on Reader connected to the workstation.

Operators shall be able to specify that any Visitor be accompanied by a specific Employee/Student, a member of a specific Group of Employee/Students, or any cardholder belonging to a specific company or department. When an operator grants accompanied access permissions to a Visitor, the system shall ensure that the Visitor’s access permissions constitute a subset of the accompanying Employee/Student’s access permissions. Operators shall also have the option to define Access Control permissions for a Visitor by attaching an Access Control template to that Visitor’s record (see paragraph detailing Access Control templates below).

3.2.4.3 IMAGE CAPTURE

It shall be possible to capture or import digitized video images and associate them with cardholder 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.

3.2.4.4 CARD PRINTING

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

3.2.4.5 ACCESS CONTROL SETUPS AND FUNCTIONALITY

3.2.4.5.1 GROUP CONTROL

It shall be possible to manage Access Control and monitor activity of Individual Cardholders and Groups of Cardholders. Group management functionality shall include the facility to administer an entire Group of Employee/Students and/or Visitors as a single entity.
Authorized Operators shall be able to specify the Zones and Readers where a cardholder 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 SMS application software shall enable administrators to assign arbitrary access levels to a Group, and override zone control and/or anti-passback control for any Group.

The SMS shall further be capable of assigning cardholders to multiple Groups.

### 3.2.4.5.2 SUPPORT FOR COMPANIES / DEPARTMENTS

It shall be possible to define any number of Separate Companies within the SMS. The software shall also provide an option enabling administrators to define Departments within each Company. The cardholder management modules shall enable operators to specify the Company and Department to which a Cardholder belongs. It shall be possible to associate one or more Employee/Students with a Company / Department by selecting the Employee/Students in the relevant cardholder management module and dragging the selection to the Company / Department management module.

When a selected subset of Employee/Students is dragged to a Company, the software shall prompt the user to select the Department to which the Employee/Students shall be assigned. It shall be possible to assign all Employee/Students in a company to a Cardholder Group by dragging an icon representing the company to an icon representing the cardholder Group. When a company is assigned to a cardholder Group in this manner, the software shall prompt the user to assign all cardholders in the company to a single Group or to create a separate Group for each Department.

### 3.2.4.5.3 ZONE CONTROL

The SMS 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, and/or selecting other Zones adjoining 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 software shall provide the capability to enforce zone control by allowing access to a zone ("inner zone") only to cardholders who have previously been allowed access to an adjoining zone ("outer zone").

The system shall also be capable of enforcing strict anti-passback control by denying access to a zone if an Employee/Student or Visitor previously entered that zone without subsequently exiting. It shall further be possible to enforce anti-passback on a time basis by denying access to or from a zone for a certain amount of time. This amount of time shall be selectable via a parameter. It shall be possible for administrators and authorised opera-tors to override the enforcement of anti-passback control for any individual cardholder or Group of cardholders.

The Zone Control application shall allow the user to view any existing Zones listed in the dialog box. A user, with proper authority, shall be able to modify, add, or delete a Zone from the System Software.

More than one Zone may be added to a Template as long as there is no overlap of a controller in a Zone already added to the Template.
Zones may be combined into Master Zones, which can then be added to a Template.

### 3.2.4.5.4 ACCESS CONTROL TEMPLATES

The software shall allow operators to assign a set of Access Control permissions to an Employee/Student or Visitor by applying a predefined template.

**Each Access Control template shall define the following parameters:**

- Company/Departments to which the template applies;
- Zone and Reader permissions;
- Schedules specifying the periods for which zone and Reader permissions are active;
- Cardholder Groups;

When a template is assigned to a cardholder, the cardholder will inherit his or her permissions from the Access Control template.

### 3.2.4.5.5 COMMAND SETS

A Command Set defines an action or actions to be sent to a controller or controllers.

**Command Sets can include:**

- Unlock and Relock a Door;
- Lockdown and Release a Lockdown on one or more doors;
- make the rest of today a Holiday;
- Mask all Interior Alarm Points;
- Change the Campus Threat Level;
- Forgive All Passback.

Once defined, a Command Set can be executed from the Command Set Window, or from a Graphic Floor plan ICON, if defined. There shall be an unlimited number of Command Sets available to be defined. Command Sets shall be defined with pick lists and shall be restrictable by Operator Group(s) and Workstation(s).

### 3.2.4.5.6 SWIPE SEQUENCING

The SMS shall enable administrators to define complex access permissions by configuring the system to require a specific sequence of up to five (5) card Reader transactions before allowing access at a Reader. For each transaction in a swipe sequence, it shall be possible to specify that a card be presented by a specific cardholder, any member of a specific Group, any cardholder with a specific access level, or any valid cardholder.

Swipe sequencing shall be integrated with the system's event and action control functionality, thus allowing administrators to configure different sets of actions for each transaction in a swipe sequence.

### 3.2.4.5.7 READER MONITORING

The system shall provide functionality for the control of monitoring devices (including CCTV cameras) based on events generated by the system in response to card Reader transactions. The SMS application software integrated with the PSIM shall provide means by which a live video signal from a CCTV system may be displayed automatically on any workstation monitor when a card is presented at a Reader or the status of any system object matches user-defined parameters. For this purpose, frame grabber interface cards shall be installed on all workstations.
designated on the drawings as monitoring stations. The frame grabber interface cards shall comply with the requirements of the SMS software vendor and shall be certified as being compatible with the computer workstation hardware and operating system.

Operators shall be able to invoke a Reader monitoring module directly from the main menu of the SMS software application. Users shall be able to select from a drop-down list any Reader defined in the system. The Reader monitoring module shall indicate the date and time of the last Access Control transaction at the selected Reader, as well as the name and photograph of the cardholder who effected the transaction. It shall be possible to access the cardholder's record in the SMS database by clicking on a button in the Reader monitoring window. Duly authorized operators shall be able to view and edit all fields in the cardholder's database record (as specified elsewhere) or remove a cardholder record from the database.

3.2.4.5.8 RANDOM EMPLOYEE/STUDENT / VISITOR SEARCH FUNCTIONALITY

Authorized Operators shall be provided with the capability to define random stop-and-search procedures at any Reader. For each Reader, it shall be possible to enable random search separately for Employee/Students and Visitors. Administrators shall be able to specify that a percentage of all cardholders, every nth person, a specific cardholder, or all members of a specific cardholder Group be searched. The random search facility shall also allow administrators to specify that a cardholder who has been identified for searching be denied access at the Reader and/or be marked for searching at other Readers where random searching has been enabled. The software shall allow administrators to assign a schedule specifying the period(s) during which random search functionality is active at a Reader.

3.2.4.5.9 VISITOR AND EMPLOYEE/STUDENT TAKE-ON STATIONS

The software vendor shall provide a cardholder take-on module that enables users with limited computing experience to view, edit and add records to the Employee/Student and Visitor database, and to assign cards to Visitors or Employee/Students.

The personnel take-on module shall provide functionality that allows operators to:

- Enter detailed information about Visitors and Employee/Students 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 Visitor or Employee/Student data record.
- Capture voice samples using a microphone connected to the take-on station, and link voice samples to specific Visitor data records.
- Ascertain the location of any Visitor or Employee/Student by displaying a list of all cardholders who have passed through access points.
- Capture images at any size ranging from 320x240 pixels to 800x600 pixels and any aspect ratio between 800:1 and 1:800. (Administrators shall have the capability to specify limits for both the pixel resolution and aspect ratio of captured images.)
- Specify that a Visitor shall be accompanied by a specific Employee/Student or any member of a specific Group of Employee/Students (such as a company or department).
- Restrict a Visitor to specified areas by assigning an Access Control template defining permissions for that Visitor (as described in the section dealing with Access Control templates).
- Specify the period for which a Visitor card is valid.
- Define templates for Visitor or Employee/Student cards and select a different template for each card.
- Print personalized Visitor and Employee/Student 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 functionality available on a personnel take-on station shall depend on permissions and configuration data assigned to a user Group by the system administrator. Operators shall be required to log on to the system by typing in a username and password, presenting their access cards, or by presenting a biometric print at a card Reader or biometric Reader which has been designated as the log-on Reader for a specific workstation (These Readers shall be attached directly to the workstation via USB or serial interface).

3.2.4.5.10 SITE CONFIGURATION

The SMS shall provide administrators with the capability to configure graphical pages that depict the layout, configuration and status of the system in real time.

Users shall have the capability to generate object-based graphical maps depicting the layout and hardware configuration of the site using an integrated vector graphics module. Additionally, users shall be able to import graphics from other applications in a range of standard formats, including BMP, JPG, TIFF and WMF.

The graphical site design module shall provide drag-and-drop definition and manipulation of Zones, Readers and other system objects. The properties of system objects and relevant relationships between them shall be configurable by clicking on graphics representing the system objects or by dragging toolbar icons to graphical objects. Once associations between graphics and system objects have been defined, operators shall be able to click on graphics (or hover the mouse pointer over them) to view properties and change settings if they have the rights to do so.

Specifically, it shall be possible to drag and drop Employee/Students or Visitors onto Zones or Readers in order to allow them access to those Zones or Readers. It shall also be possible to animate graphics on status monitoring pages in real time by controlling the properties of related data objects in response to real-time events generated in the system.

3.2.4.5.11 OBJECT AND EVENT CONTROL

The SMS software shall provide the capability to define dynamic objects representing any device linked to the system. Administrators shall have the capability to control the behavior of objects defined in the SMS in response to real-time events generated by devices linked to the system.

The object model employed by the SMS shall be sufficiently generic to support a full spectrum of security devices, including but not limited to Zones, doors, Readers, controller input and output points, timers, counters, turnstiles, booths, smart doors, operator stations, and drop boxes.

An event and action configuration module shall be provided to enable users to set up actions in response to system events or the status of system objects. Typically (and as a minimum requirement) the event and action configuration module shall allow users to monitor the status of digital input points and control the behavior of digital output points defined on controllers linked to the host computer. The SMS shall also provide the capability to control and respond to the behavior of “virtual” (i.e. memory-based) input and output points. System objects representing virtual I/O points shall provide methods to define the behavior of those I/O points by toggling, simple pulsing, and pulsing on and off repetitively for specific durations to set up “pulse trains”.

Users shall have the ability to define sequences of actions that are executed at system startup in order to restore the SMS to a valid state in the event of a system reboot being necessary.

3.2.4.5.12 SYSTEM ALARM MANAGEMENT

The SMS software shall provide tools for the configuration, monitoring and management of system alarms. Wherever possible, system objects shall incorporate the capability to raise alarms.
when specific events occur. Administrators shall be able to specify the severity level of any alarm as “critical”, “normal” or “low”, enable or disable an alarm, and configure an alarm to reset automatically. Operators shall have access to an alarm viewer that displays the status of active alarms in real time, and allows alarms to be acknowledged or reset. It shall be possible to define actions that are executed when alarms are raised by the system, acknowledged or reset by an operator, or automatically reset by the system. In addition, the system shall allow an operator to attach a schedule (as described elsewhere in this specification) to an alarm in order to specify the time period(s) for which an alarm remains enabled.

3.2.4.5.13 SYSTEM MONITORING

The SMS 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, system events, video inputs, the current location of cardholders, key system statistics, and system performance.

The Access Control Event Viewer shall list the last n (“n” specified by user) Access Control Events that have been logged in the SMS database. Users shall be able to select which properties of an Event are displayed and in which order they are displayed.

The System Event Viewer shall list the last n (“n” specified by user) System Events that have been logged in the SMS database. Users shall be able to select which properties of an Event are displayed and in which order they are displayed.

A video viewer shall enable users to monitor Video Signals from the CCTV system (PSIM integration).

A personnel locations viewer shall be provided to enable operators to ascertain the current location of any cardholder. This viewer shall provide information about the last Reader at which a cardholder presented their card, or the last zone that the cardholder entered.

The system performance monitor shall allow users to set up real-time 2-dimensional or 3-dimensional graphical representations of transactions at any ID Reader(s) defined in the system. It shall be possible to filter the data represented in a graph by selecting a day from a graphical calendar and selecting specific one-hour periods within that day. Users shall also be able selectively to display “access allowed” events, “access denied” events and “all events” in different colours. Additionally, users shall be able to preview and print reports by clicking on an icon in the performance monitor.

3.2.4.5.14 INTRUSION ALARM CONTROL

The SMS shall allow users to define an unlimited number of independent intrusion alarm systems, each comprising one or more user-defined alarm Zones. It shall be possible to link any available digital input point to any alarm zone and to employ any such input point as an alarm trigger. It shall be possible to raise an intrusion alarm event in response to the status of any input point, or any valid combination of object properties. The system shall allow any alarm zone to be specified as an entry/exit zone for an intrusion alarm system associated with that alarm zone. Administrators shall have the ability to specify arming/disarming codes and duress codes at any Reader that is equipped with a keypad and is set up in the system as an intrusion alarm arming/disarming station. When a duress code is entered at a terminal, the system shall automatically raise a duress alarm event and display an appropriate message on client workstations that are used to monitor that terminal. The system shall allow the configuration of panic inputs, i.e. alarm points that remain active regardless of whether the intrusion alarm system is armed or disarmed. The software shall allow administrators to enable the arming of an alarm zone in response to any valid sequence of system events, including the presentation of a specified access card or the entry of a specified keystroke sequence at a specified Reader. Administrators
shall be able to configure automatic arming and disarming of an intrusion alarm system by attaching appropriate schedules to the intrusion alarm system. When an intrusion alarm zone is in an armed state, the system shall allow access to the zone only to personnel who are authorized to activate/deactivate the alarm system.

3.2.4.5.15 OFFLINE FUNCTIONALITY

The SMS shall incorporate a module that enables administrators to set the system up for Access Control in offline mode. The offline management module shall interface with the SMS database to extract a subset of data required to ensure continued Access Control functionality if the communication between a Door Controller and the host computer is interrupted for any reason. While the line of communication between the host computer and the Door Controller remains operational, the data required for offline Access Control shall be downloaded to Door Controllers according to user-definable schedules. Download schedules shall provide the capability to control the update interval for each Door Controller.

As mentioned in the section of this specification pertaining to hardware, the Door Controller shall have the capability to detect a break in the line of communication to the host computer, switch automatically to offline mode, and switch back to online mode as soon as communication with the host is restored.

When communication between the host computer and a Door Controller is restored, the offline Access Control management module shall retrieve the transaction logs maintained by the Door Controller in offline mode, and upload the retrieved data to the central SMS database.

3.2.4.6 USER INTERFACE

3.2.4.6.1 SEARCH

The SMS shall provide a simple search for all Events on the Access Control Server(s). The user selects the required search period.

Once the time criterion is entered, the “search” is selected. Events during the selected period will be returned by the search. The user shall be able to search on combinations of doors, sensors or cameras by clicking on an “Advanced Search” icon as described in the next section.

Search functionality shall be available in each viewer window.

3.2.4.6.1.1 ADVANCED SEARCH

The SMS shall provide an advanced search of Events. The search shall be based on the time and Event took place and Door details. The User shall select from the list of Doors on the Access Control Server(s).

The time criteria shall be selected from a calendar and time line control. Days containing Events shall be shown in bold on the calendar control. Doors shall be able to be added and removed from the search list.

The user shall be able to choose to filter the search based on the following criteria:

- Alarm or Event Type;
- Event Severity (Low, Medium, High, all);
- Area;
- Location Name;
- Event Description;
- Operator Name;
- Door Name or Number;
Employee/Student Name;
Visitor Name.

3.2.4.6.1.2 SEARCH RESULTS

The SMS shall show the Search Results of the basic and advanced searches in a table format, such that the user is able to select columns within the list to sort the output.

Functionality shall be provided to allow the user to see a list of Events for a Door from the past 24 hours without needing to use one of the searches.

3.2.4.6.2 STATUS VIEWER

There shall be a Status Viewer which displays in a spreadsheets type format, the real-time status of all or selected Doors, Readers, Inputs, Relays, Expansion Inputs, Expansion Relays. Devices may be grouped in to “Status Groups”, which are selectable from a drop down list. Devices may have selected information displayed.

The available list includes the following:

- Name and Address;
- Status;
- Alarm and Acknowledged Status;
- Masking Status;
- Line Module Input Status and Type;
- Relay Status;
- Revision Number;
- Enabled Status;
- Controller Alarm Relay, Tamper, and Battery Status.

3.2.4.6.3 ALARM VIEWER

The Alarm Viewer shall have 4 panes: Alarm, Acknowledged Alarms, Instructions, and Comments. At the bottom of the Main Console display are counters to indicate Active Alarms, Acknowledged Alarms, and Off Normal Conditions. Double clicking the Counter will launch the Alarm Viewer. The Alarm Viewer may also be manually launched, or automatically in the event of a new alarm occurrence.

Alarm Viewer properties that may be configured include:

- Require Acknowledgement Before Clearing;
- Auto Acknowledge on RTN (Return to Normal);
- Require Entry of Note on Acknowledgement;
- Force New Note on Multiple Acknowledgements;
- Require Entry of Note on Clear;
- Force New Note on Multiple Clear;
- Restore Alarm Viewer on New Alarm;
- Specify the number of Cached Alarms to Load at Launch of Alarm Viewer.

Foreground, Background, Alarm, and Secure colors may be changed. In addition, the Columns of data viewed in the Alarm and Acknowledged windows may be selected and the sequence in which they will appear.

The available columns include:

- ICON;
Video Recorder - Video; Count; Controller Time; Host Time; Description; Address; Level; Alarm ID; Acknowledge Time and Acknowledged By (available for the Acknowledged Pane).

**Tool bar ICONS shall include:**

- Acknowledge Selected;
- Clear Selected;
- Acknowledge All;
- Clear All;
- Add Note.

**Right Clicking an Alarm Event shall display a list of available options, including:**

- Acknowledge;
- Clear;
- Acknowledge All;
- Clear All;
- Record Note;
- Go To Graphic;
- Display User Photo;
- Replay WAV file;
- Video Recorder Alarm Video: Show Viewer and Get Recorded Alarm Video.

### 3.2.4.6.4 EVENT VIEWER

The Event Viewer can display all or Filtered Transactions. Custom filers may be defined and selected, or Standard selections can be made for main categories of Event types. Column width, order, selection, and scrolling direction are user definable, as well as text and background color.

The number of cached events to load when launched, up to 10,000, may be defined. The Operator shall be able to scroll back in time to view events no longer seen on the screen, without the need for running a report.

### 3.2.4.6.5 BROWSER

There shall be a Internet Explorer like "Browser" for accessing on-line help, tutorials (WMV files), manuals, Known Issues, and Product Registration information.

### 3.2.4.6.6 CUSTOMIZATION MANAGER

There shall be a Customization Manager that allows the Operator to define an alternate language or change the English name or label for each element of the software.
Audio WAV files may be defined for playback when a particular Alarm Type is active.
Priority Levels may be defined (1-99) for each Alarm Type.
Operator Instructions per Alarm Type shall be user definable.

### 3.2.4.6.7 REPORT MANAGER
The Report Manager shall allow the Operator to select from a number of pre-defined Reports. Custom Reports can be created outside the software, and added to a Custom folder, making the Custom Reports available from within the Report Manager application.

Once a Report is selected, the default Criteria and Sorting options may be used, or custom Criteria and Sorting options may be selected.

Once the report is run, it may be viewed, printed, or saved in various standard file formats.

**Standard Reports included as standard shall include:**

### 3.2.4.6.7.1 CUSTOMIZATION REPORTS

- Component Resources;
- Customizations Report.

### 3.2.4.6.7.2 ACCESS CONTROLLER CONFIGURATION

- Controllers;
- Doors;
- Expansion Inputs;
- Expansion Relays;
- Inputs;
- Network Layout;
- Printers;
- Readers;
- Relays.

### 3.2.4.6.7.3 HISTORY LOGS

- Active Alarms by Date;
- Alarm Log by Date;
- Alarm Log by Date with Comments;
- All Events Log;
- External Events Log;
- Internal Events Log;
- Operator Log;
- User Activity Log.

### 3.2.4.6.7.4 PERSON INFORMATION

- Template Status;
- Door Access by Person;
- Dossier Style by Person;
- Expired and To-Be-Expired Person Access;
- Expired Templates;
- Last Access by Person;
- Person Access by Door;
- Person Access Summary;
- Person Access Summary with Codes and Cards;

### 3.2.4.6.7.5 SMS CONFIGURATION

- Command Sets;
- Door Groups;
Holiday Schedules;
Holidays;
Master Door Groups;
Master Door Groups with Persons;
Operator Groups;
Operators;
Time Zones – Grand Master Schedules;
Time Zones – Master Schedules;
Time Zones – Standard Schedules;
Time Zones – Standard Schedules in Use.

3.2.4.6.8 GRAPHICS

The Graphics application shall allow the Operator to add, delete or modify graphic floor plans and add indicator ICONs to graphic floor plans that represent Controllers, input/output points, readers, or cameras located in the Campus. Formats for Graphics supported shall include: jpg; bmp; dxf; wmf; emf.

There shall be two Modes, Live and Design. The Live mode shall be used for real time monitoring. In addition, right clicking an ICON presents the Operator with a list of available Access or Control Functions that can be issued to the device. The Design mode allows the Operator to Define which Graphics are to be used, place ICONs on the Graphics, and define properties for each ICON.

There shall be a Pan and Zoom Viewer that provides a key plan that can be panned and scrolled by moving the red box, which indicates the current viewing area.

There shall be a Directory of available Graphics to easily select the desired Graphic to display.

The Graphics application shall display the real-time state and condition of Alarm Points and Doors. The Door ICONs shall change from a closed door ICON to an Open door ICON, representing that the door is open. When the door is closed, a closed ICON will appear again. The Alarm ICONs shall change from a closed contact ICON to an Open contact ICON, representing that the alarm device is active. When the Alarm Device is restored to its normal condition, a closed contact ICON will appear again. The ICON will also display the Device Name and Alarm Condition that caused it to go into an Alarm condition. The Color of the ICON will also change based on whether it is in alarm or secure.

User definable ICONs can be created and used. Link ICONs can added to quickly link to other graphics. Command Set ICONs can be used to issue a Command Set with a single mouse click.

3.2.4.6.9 BADGE AND GRAPHICS DESIGNER

The Badge and Graphics Designer shall allow the Operator to create and customize an unlimited number of Badge Templates that may be assigned to a Person in the Enrollment Manager and create Backdrops to be used in the Graphics module.

An Object Toolbar shall be available for selecting Objects to appear on the Badge Template or Backdrop, including: Bit Map Logos, Photos, Fixed Text, and Database Fields. Each Object shall have a Properties box where the specific Properties of that Object are defined, including: File, database field, Font Color, Font Style, Font Size.

3.2.4.6.10 ENROLMENT MANAGER

The Enrolment Manager application shall maintain information related to a Person, and Credentials assigned to that person. Multiple Credentials per person shall be supported. The list...
of People shall be able to have Custom filters applied, allowing for quick and easy grouping of
desired people. There shall be a quick find option for finding a specific person or credential.

The Personal Information pane shall include the General and 10 Additional Tabs. The system shall
be capable of defining an unlimited number of user definable fields and place them on any of the
10 Tabs. The captions of the Tabs are customizable and can be restricted by Operator. These
field names can be either a "Text Box", "Dropdown" where the Operator can enter text, or select
from a Dropdown List, a "Dropdown List" where selecting from the List is required, and the
Dropdown and Dropdown Lists can sort in Ascending or Descending order. Fields can be made
"Required", where the Person's record cannot be saved unless data is entered in that field. Field
captions can have their color changed. A Photo field shall be available for acquiring a live video
image, acquire an image from a TWAIN device, or acquiring a photo from an existing file. A
Record Last Updated field shall be available, as well as Preview and Print a Badge. A signature
field shall also be available.

Once a person is added, one or more Credentials may be added to that Person. Credentials may
be added using a Credential Template, or directly without a Credential Template. The Credential
will take on the properties of the Credential Template if used. There shall be a Card Enrollment
Station used for entering card data into the system. PIN Numbers can either be randomly
selected, or Operator/User selected.

Once a Person is selected from the List, the Credential Status and information is displayed for the
assigned Credentials. The information includes: IDF, ID, Function, Description, Status, Expires
On, Last Access, Last Door, Tag, and Alert. An Operator may right click on a Credential, and will
be presented with the following options: Tag, Alert, Disable, Forgive Passback, Override Code

The bottom of the Enrolment Manager window shall display counters for: People, Assigned
Credentials, Unassigned Credentials, and Guest Credentials.

3.2.4.6.11 SWITCH OPERATOR

There shall be the capability to change Operators without the need for the current Operator to
Log Off the computer. The new Operator’s SMS permissions are then used during the session to
control access to SMS functionality.

3.2.4.6.12 ADD-INS

The following “Add-Ins” are available to be added to SMS by an authorized Operator.

**SMS Remote Desktop** – The Operator shall be able to launch a terminal services session from
within the SMS shell.

**Launchpad** – The Operator shall be able to launch standard Windows applications within SMS.

3.2.4.7 SCHEDULING AND TIMING

3.2.4.7.1 COUNTERS

The SMS 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 as well
as three (3) set points for each counter. For each set point, it shall be possible to define actions
that are performed by the system when the counter is less than, equal to or greater than that set
point. 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 to an
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.

### 3.2.4.7.2 TASK SCHEDULER

There shall be a Task Scheduler that allows functions to be performed on an as needed basis, like Activating and Deactivating Templates. It can also schedule Tasks like: Synchronize Controller Clocks; Run Historical Log Archiver; Run Reports; Import/Export User Data; Execute third party applications; Dial-Up remote sites; and Run Command Sets on a Daily, Weekly, Monthly basis. The scheduler shall allow the Operator to schedule tasks in time frames of milliseconds through years.

### 3.2.4.7.3 ACCESS CONTROL SCHEDULES

The SMS 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 Access Control Templates, Zone Permissions or Reader Permissions for any Cardholder or Group of Cardholders.

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.

In addition to Monday-Sunday, there shall be one day of the week called Holiday. When selected, there will be 4 Holiday Schedules that determine if the Holiday is to be followed for this Access Control Schedule.

There shall be at least 50 Standard Access Control Schedules, 50 Master Access Control Schedules and 20 Grand Master Access Control Schedules.

### 3.2.4.7.4 HOLIDAYS

Holidays are used within the system for the purpose of defining if an Access Control Schedule is to be followed on a defined Holiday. Each Time Zone has up to 4 Holiday schedules. There are 366 user definable Holidays this year and 366 days next year.

It shall be possible for the Operator to “Make the rest of Today a Holiday”.

### 3.2.4.8 REPORTING

#### 3.2.4.8.1 REPORT GENERATION

It shall be possible for authorized users to extract detailed reports from the SMS without running the main software application. The software vendor shall provide a separate reporting module for this purpose. The reporting module shall be able to be executed from any PC with a TCP/IP connection to the host computer on which the SMS is installed.

At a minimum, it shall be possible to generate the following reports:

- Access Control Events;
- System Events;
Basic Time and Attendance;
Locations of Cardholders;
Employee/Student Details;
Employee/Student Summary;
Visitor Details;
Visitor Summary;
Company Details;
Company Summary;
Zone Details;
Zone Summary;
Door Details;
Door Summary;
ID Reader Details;
ID Reader Summary;
Digital Input Details;
Digital Input Summary;
Digital Output Details;
Digital Output Summary;
Timer Details;
Timer Summary;
Drop Box Details;
Drop Box Summary;
Operator Station Details;
Operator Station Summary;
3.2.4.8.2 SCHEDULE DETAILS.

The SMS shall further supply an open interface the CLIENT (or his/her IT personnel with the necessary knowledge) to obtain any additional reports or time and attendance data without having to go back to the installer or SMS supplier to have every new report programmed into the system. The SMS shall as a minimum interface to a third party program like Crystal Reports.

3.2.4.8.3 TIME AND ATTENDANCE FUNCTIONALITY

The SMS software application shall incorporate support for the acquisition, recording, reporting and exporting of basic time and attendance data for all cardholders.

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 cardholder Group or individual cardholder.

Integrated reporting functionality shall enable users to extract basic time and attendance reports from the SMS database. Users shall be able to construct database queries by selecting or deselecting options in a pop-up window which can be invoked from the report viewer. It shall be possible to specify date ranges, specific Employee/Students, Employee/Students of specific companies and/or departments, specific Visitors, Visitors to specific companies and/or departments, cardholder Groups, and system Readers for inclusion in a time and attendance report. The time and attendance report shall include (for each time and attendance period) the surname and first name of the cardholder, the time and date when the cardholder clocked in, the Reader at which they clocked in, the time and date when the cardholder clocked out, the Reader at which they clocked out, the length of time that elapsed between clocking in and clocking out, the company/department where the cardholder clocked in and out, and the type of cardholder (Employee/Student or Visitor).

In addition to the minimum time and attendance data reporting functionality outlined above, the SMS software shall provide the capability to filter time and attendance data by specifying that time and attendance periods shall be reported only for Employee/Students who have worked more than a certain number of hours per day. It shall be possible to ignore clocking transactions that are less than a specified number of minutes apart, and to round time and attendance periods to a specified number of minutes (e.g. to the nearest 1/5/10/15/30/60 minutes).

The SMS 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.

3.2.4.9 DATA HANDLING

3.2.4.9.1 DATA ADMINISTRATION AND BACKUP

Users shall have the ability to import Employee/Student and Visitor data from a variety of standard data sources. 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 SMS shall provide tools that enable users to verify and maintain the integrity of the system database. The data integrity tools shall identify invalid schedules, Employee/Students belonging to more than one Group, duplicate input or output addresses, and connections to addresses on undefined Readers.

The software vendor shall provide tools that allow system data to be backed up and restored manually and automatically. The SMS shall use a Standard Archiving Method to backup data.
The automatic backup facility shall allow the user to select when data is backed up in at least the following ways:

At a specified time:
- Of the day;
- Of the week;
- Of the month;
- Etc.

When a specific event occurs in any system linked to the SMS (e.g. General Fire Alarm);
If there are more than a specific number of events in the database (e.g. 1,000,000 events);
When the storage space on the Server crosses a pre-defined threshold the SMS shall backup to an Offline storage medium.

3.2.4.9.2 OFFLINE STORAGE

The SMS shall be able to manage several Off-Line Media Devices for Archiving and Restoring the Event Database. The SMS shall use a Standard Archiving Method such as Microsoft Remote Storage Services to handle offline media.

All of the following Off-Line devices shall be supported:

- Standard CD Writer or Robotic CD Unit;
- Standard DVD Writer or Robotic DVD Unit;
- Standard DAT Drive or Robotic DAT Unit.
- A folder on another PC / Server connected to the network where it shall be possible to set the IP address and a specified folder as well as size limitations for the backup.

If a user attempts to access Data Stored in Off-Line Media then the SMS will automatically restore and make the data available if it is accessible to the Robotic CD/DVD/DAT Unit, or shall prompt the User the make the Media containing the data available to the Archive Device.

3.2.4.9.3 DATABASE SIZE LIMITATION SETTINGS

The SMS shall allow the user to set a limit on the database. It shall be capable of limiting the size of the database in at least the following manners:

- A percentage of the available Hard drive / Backup media space (e.g. 75% of the available HDD space = 2TB);
- A certain amount of pre-defined HDD space (e.g. 500GB);
- A certain number of pre-defined Events in the database (e.g. 1,000,000,000 events).

3.2.4.9.4 LOW STORAGE SPACE WARNINGS

The SMS shall inform the user / CLIENT of any impending problems with low storage space on any media used as a backup medium.

The SMS shall be capable of warning the client in at least the following manners:

- Via on-screen warning messages to the Operators / Users;
- Via GPRS modem: "SMS" or "MMS" to predefined cellphone numbers (future);
- Via email to predefined email addresses;
3.2.4.9.5 SQL DATABASE MANAGER

The SQL Database Manager shall be used to Backup and Restore data from the SQL database. Manual or automatic backups may be defined. SQL Scripts may also be run from the SQL Database Manager Query Tool against the Event Database.
ACCESS CONTROL HARDWARE

4.1 GENERAL

Access Control Doors will be installed in security areas where personnel move and work. The locations will be indicated on the Engineers Drawings.

4.2 DEFINITIONS

**Online Access Control:** Where Access Control Hardware (Card Readers, Biometric Readers, Green Breakglass Units, Door Position Switches, Key Overrides, and Electro-Mechanical or Magnetic Locks) are installed in provisions around a door and hard wired back to a controller. Real time information is available from the system.

**Escutcheons:** Electronic Locksets, with Built-in Card Reader(s) and a Handle. The Escutcheon can communicate through "Data-on-Card" or through a wireless network.

**GEO E-Cylinder:** Electronic E-Cylinder (Euro Profile or Oval), with Built-in Card Reader(s) and a Handle. The GEO Cylinder can communicate through "Data-on-Card" or through a wireless network.

**Standalone Access Control (SAC):** The (Escutcheon, E-Cylinder, E-Glass Door Lock, E-Padlock and/or E-Panic Device) contains all hardware needed for an Access Control Door.

**Semi-Online Access Control:** When a SAC uses a wireless network to communicate back to the Access Control System we define this as semi-online, because the wireless network can go offline or be blocked. When the wireless network is operational real time information is available from the system. The system will operate with "Data-on-Card" as a backup communications medium.

**Offline Access Control:** When a SAC uses "Data-on-Card" to communicate back to the Access Control System we define this as Online, because the data may not be transferred from the Online Readers to the correct Offline devices via the "Data-on-Card". No real time information is available.

**Wireless:** Semi-Online battery powered SAC (Escutcheon, E-Cylinder, E-Glass Door Lock, E-Padlock and/or E-Panic Device).

**Wireless Ready:** The SAC shall be upgradable by adding an antenna to the inside board without upgrading the firmware or adding any batteries.

**Portable Programmer Device (PPD):** A PPD is used to program new locks for the first time or power locks where the battery has run down without being replaced.

**Virtual Network (VN):** The distribution of information throughout the system using "Data-on-Card" is defined as the Virtual Network. Information is distributed through the system like a virus by the card holders.

4.3 SYSTEM DESCRIPTION

Depending on the level of security, the system shall consist of Online, Semi-Online and Offline Doors. The will be indicated on the Engineers Drawings.

"Data-on-Card": The Access Plan of each User should be stored on the Card as well as on the Controllers or the SACs.

**Virtual Network**:
- The SAC should be able to:
  - Write the Audit Trail on the User Card(s).
  - Write the Battery Status on the User Card(s).
  - Eliminate Blacklisted Users Card(s).
- The Controller should be able to:
  - Update the Access Plan on the User Card.
  - Revalidate the User Cards (by hours or days).
  - Read the Audit Trail of Each User Card and Transmit it to the Server.
▪ Read the Battery Status Stored on a User Card and Transmit it to the Server.
▪ Transmit all Black Listed Users to the Cards.

The same Software shall monitor the three (3) types of Access Control Systems (Online, Semi-Online and Offline) and all the Accessories. The same platform will handle for all the three (3) types of Access Control. The Access Control System shall be an IP based system, configured on LAN or WAN protocols.

Tenderers to note that a number of Sallis (by SALTO) locks have already been procured though the building contracts, integration to these locks is mandatory.

4.3.1 RFID TECHNOLOGY

Provide single technology contactless smart cards complying with ISO 14443A or B, under 13,56 MHz
Presentation to an access reader at any angle within a minimum of 50mm shall result in an accurate reading of the card.
Support read/write capability, with a minimum of 1 Kbytes Data retention rate shall be 10 year nominal.
Suitable for direct two-sided dye-sublimation or thermal transfer printing.
Chip enabled to store accounting information for third party devices.
The number of Access Cards to be provided will be indicated in the Bills of Quantities.
Approved RFID Manufacturers:
• DESFire EV1 (NXP)

Offline Access Control:

Is composed of a Battery Operated Escutcheons, E-Cylinders, Glass Door Locks and/or Panic Devices with Mortise Locks & Strikes. When an RFID Card is Presented it will Activate the Handle to Retract the Latch.
The SAC shall work in a Virtual Network Environment in Combination with the Online System.

With the minimum requirements:

The SAC Devices shall Write the Audit Trail of Each Transaction on the Card;
The SAC Devices shall Write its Battery Status on the Card that is Presented;
The Card shall Transmit the Black List to the SAC;
The SAC Devices shall Read the Validation of the Card;
The SAC Devices shall Read the Access Plan situated on the Card and Grant or Deny the Access Accordingly.

4.3.2 ESCUTCHEON

The Escutcheons shall comply with the following specifications:

Material : 304 Stainless Steel;
All fixing screws shall be concealed for greater security and improved aesthetics;
Must have an Electronic Privacy Button from Inside.

Battery Powered:
- 3 X Standard Alkaline Batteries - LR03 – AAA, 1.5 V;
- Optional 3 x Lithium Batteries - FR03 – AAA, 1.5 V.
- Minimum Number of Openings on a Set of Batteries:
  ▪ 40,000 for a Semi-Online SAC;
  ▪ 60,000 for an Offline SAC.
- Low battery power indication monitored through the Wireless Network or the Virtual Network (VN) and passed to the software. Also readings can be taken at the lock and passed to the software via PPD connection.

Indication:
- Dual colour LED (green / red) to indicate Access Authorization;
- Sounder to indicate Access Authorization;
- Different Sound and Light Indication when Card is presented if rejected or accepted.

Environmental conditions:
- Temperature Range: - 20 ºC to 70 ºC;
- IP Protection Rating: IP55.

Certifications:
- Highest EN Certifications;
- UL 10C compliant (180 min steel doors, 90 min wooden doors);
- EN1634-2 EI 120 Fire Resistant.

Access Control Features:
- Maximum number of users per door: 4 000 000;
- Maximum number of doors in a system: 64000;
- Maximum events on lock audit: 1000;
- Time zones: 256;
- Time periods: 1024;
- Calendars in system: 256;
- Zones in system: 1024;
- User groups: unlimited;
- Anti-Passback.

Available Lock Modes:
- Standard Mode (Locked at all Times);
- Office Mode (Free Passage);
- Timed Office Mode (Automatic Locking at End Time);
- Automatic Opening Mode (8-Pairs of "Hands Free" timed Lock and Unlocks per day with Holidays);
- Toggle Mode (Present Card to Lock, Present Card to Unlock);
- Timed Toggle Mode (Present Card to Lock, Present Card to Unlock depending on Schedules).
- Emergency Opening by means of the PPD;
- Non-volatile memory (memory is not deleted, even if power fails);
- Firmware shall be upgradable through the PPD;
- Simple off-line installation shall be possible on any type of door, including those with narrow frames;
- All communications between the carrier and the SAC shall be encrypted and secured;
- High security via high resistance, hardened anti-drill protection;

Minimum Features for a Semi-Online (Wireless System):
- Door Status;
- Door Opened;
- Door Closed;
- Door Left Open;
- Intrusion.
- Re-Rooming;
- Instant Extended the Validity of the Card;
- Online Staff/Student Tracking;

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
• Real Time Monitoring;
• Instant Card Cancellation;
• Dynamic Master Keys;
• Privacy Mode Monitoring;
• Real Time Audit Trail;
• Automated “Low Battery Report”;
• Real Time Audit of Inside Openings;
• Optional Real Time Mechanical Override Audit;
• Passage Mode Activates for Meeting Rooms;
• Lost Card Cancellation;
• Fully Featured Access Control Software Module;
• Maintenance Management (Different Cards to Indicate Different Problem in the Room).

4.3.3 GEO E-CYLINDER

Extensive range of compact sized electronic cylinders for doors where fitting an electronic escutcheon is not possible or required. Available in different models, e.g. half cylinder, cylinder with thumb turn, double cylinder, cam lock cylinder, padlock, and with a wide offering of different profiles, e.g., Euro, UK oval, Swiss Round, Australian oval, Scandinavian and ANSI.

The GEO E-Cylinder shall comply with the following specifications:

Material : 304 Stainless Steel;
All fixing screws shall be concealed for greater security and improved aesthetics;
Available Models:
• Half Cylinder;
• Half Cylinder with Thumb-Turn from Inside;
• Double Cylinder;
• Rim Type Cylinder.
Available CAM Cylinder Profiles:
• Euro Profile;
• Swiss Round Profile (RP22);
• UK Oval Profile;
• ANSI US;
• Australian.
Available Finishes:
• Satin Nickel;
• Satin Chrome;
• Polished Chrome;
• Polished Brass;
• Brown Platinised;
• Black Platinised.
It shall be possible to have all Cylinders numbered.
The E-cylinder can always be opened from the inside (a single action panic feature works in conjunction with the relevant mortise lock).
Battery Powered:
• 1 x Standard Lithium Battery - CR2, 3.0 V (IEC: CR17355);
• Minimum Number of Openings on a Set of Batteries:
  ▪ 30,000 for a Semi-Online SAC;
  ▪ 50,000 for an Offline SAC.
- Low battery power indication monitored through the Wireless Network or the Virtual Network (VN) and passed to the software. Also readings can be taken at the lock and passed to the software via PPD connection.

**Indication:**
- Dual colour LED (green / red) to indicate Access Authorization;
- Sounder to indicate Access Authorization;
- Different Sound and Light Indication when Card is presented if rejected or accepted.

**Environmental Conditions:**
- Temperature Range : - 20 ºC to 65 ºC;
- IP Protection Rating : IP55 or IP66 on request.

**Certifications:**
- SKG compliant;
- VdS BZ+ approval models shall be available.
- UL 10C compliant (180 min steel doors, 90 min wooden doors);
- EN1634-1 EI 60 Fire Resistant.

**Access Control Features:**
- Maximum number of users per door: 4,000,000;
- Maximum number of doors in a system: 64,000;
- Maximum events on lock audit: 1000;
- Time zones: 256;
- Time periods: 1024;
- Calendars in system: 256;
- Zones in system: 1024;
- User groups: unlimited;
- Anti-Passback.

**Available Lock Modes:**
- Standard Mode (Locked at all Times);
- Automatic Opening Mode (8-Pairs of “Hands Free” timed Lock and Unlocks per day with Holidays);
- Toggle Mode (Present Card to Lock, Present Card to Unlock);
- Timed Toggle Mode (Present Card to Lock, Present Card to Unlock depending on Schedules).
- Emergency Opening by means of the PPD;
- Non-volatile memory (memory is not deleted, even if power fails);
- Firmware shall be upgradable through the PPD;
- Simple off-line installation shall be possible on any type of door, including those with narrow frames;
- All communications between the carrier and the SAC shall be encrypted and secured;
- High security via high resistance, hardened anti-drill protection.

**Minimum Features for a Semi-Online (Wireless System):**
- Re-Rooming;
- Instant Extended the Validity of the Card;
- Online Staff/Student Tracking;
- Real Time Monitoring;
- Instant Card Cancellation;
- Dynamic Master Keys;
- Privacy Mode Monitoring;
- Real Time Audit Trail;
- Automated “Low Battery Report”;
- Real Time Audit of Inside Openings;
- Optional Real Time Mechanical Override Audit;
- Passage Mode Activates for Meeting Rooms;
- Lost Card Cancellation;
- Fully Featured Access Control Software Module;
- Maintenance Management (Different Cards to Indicate Different Problem in the Room).
4.3.4 LOCKER LOCK

Locker Lock should be designed to bring all the Advantages of an Electronic Access Control for Locker, and Cabinets.

The Locker Lock shall comply with the following specifications:

Material: Plastic Cover Characteristics:
- Highly Resistant to:
  - Chemicals;
  - UV Radiation;
  - Physical Impacts.
Cover Colour: RAL 7016 - Antracit.
Internal Locking Components:
- Mechanical Components located on the inside and made of steel;
- Surface Mounted Lock;
- Sandwich Construction with the Reader on the Outside and Lock Case on the Inside;
Typical Inside Cover Dimensions: 100 mm x 110 mm x 25 mm.
Typical Outside Escutcheon Dimensions: 55 mm x 105 mm x 28 mm.
Typical Deadbolt Projection: 15 mm.
Outer Thumb-Turn shall have a Red-Green indicator for availability of the locker with an electronically managed release.
All fixing screws shall be concealed for greater security and improved aesthetics;
Its ergonomic frontal knob has to be designed to make easier the use of the locker.
The electronic and the mechanical components should be located on the inside to enhance the security against vandalism or manipulation.
The locker should be simple and intuitive use and the possibilities that the key can have any shape to make this system a good option for your special needs.
The locker should be able to control access to lockers, cupboards, cabinets, cabins, and boxes, show cases, where access control and full audit trailing are required.
Battery Powered:
- 3 x Standard Alkaline Batteries - LR03 – AAA, 1.5 V;
- Optional 3 x Standard Lithium Batteries - FR03 – AAA, 1.5 V.
- Minimum Number of Openings on a Set of Batteries:
  - 60,000 for an Offline SAC.
  - Low battery power indication monitored through the Wireless Network or the Virtual Network (VN) and passed to the software. Also readings can be taken at the lock and passed to the software via PPD connection.
Indication:
- Dual colour LED (green / red) to indicate Access Authorization;
- Sounder to indicate Access Authorization;
- Different Sound and Light Indication when Card is presented if rejected or accepted.
Environmental conditions:
- Temperature Range: - 20 ºC to 70 ºC;
- IP Protection Rating: IP55.
Certifications:
- EN 60529.
Access Control Features:
- Maximum number of users per door: 4 000 000;
- Maximum number of doors in a system: 64000;
• Maximum events on lock audit: 1000;
• Time zones: 256;
• Time periods: 1024;
• Calendars in system: 256;
• Zones in system: 1024;
• User groups: unlimited;
• Anti-Passback.

Available Lock Modes:
• Fixed Locker Assignment where a specific ID Carrier Operates a Specific Lock.
• Free Locker Assignment where any ID Carrier Subsequently used to Unlock a Locker Takes Control.
• Family Option - Allows for Multiple ID Carriers to Operate a Single Locker.

Emergency Opening by means of the PPD;
Non-volatile memory (memory is not deleted, even if power fails);
Firmware shall be upgradable through the PPD;
Simple off-line installation shall be possible on any type of door, including those with narrow frames;
All communications between the carrier and the SAC shall be encrypted and secured;
High security via high resistance, hardened anti-drill protection.

4.3.5 WIDE PROFILE MORTISE LOCK & STRIKE

EURO lock (axe distances 85mm.)
Euro lock is a mortise lock with latch projection which means the latch is automatically projected and deadlocked when the door is closed. This mortise lock is suitable for all kinds of wooden door whether it’s a hotel room, office or warehouse door etc. The latch projection function increases security by making it impossible to gain access by using plastic cards.

For additional security the option to order this lock with a deadbolt shall be available.

The Wide Profile Mortise Lock & Strike shall comply with the following specifications:

- Lock Case, Latch and Deadbolt made of Steel;
- Axes Distances: 85mm;
- 8mm Square Spindle;
- Turning Angle 30º;
- Different Backsets;
- Available CAM Cylinder Profiles:
  • Euro Profile;
  • UK Oval Profile;
- Available Finishes:
  • Satin Stainless Steel;
  • Gold Enamelled.
- Reversible Latch and Auxiliary Latch (Anticard).
- With Auxiliary Latch (Anticard) it Deadlocks the Latch.
- Handle Retracts the Latch to Normal Position.
- Panic Function Option (Handle Retracts the Latch and the Deadbolt).
- Deadbolt Detector Option for Electronic Privacy Function.
Mortise Lock EN 12209 Grade 3 (High Frequency of Use or With Care, Use in Public Buildings).
Mortise Lock EN179 Grade 3* (Suitable for Use in Busy, High Traffic Areas).
EN-1634-1 Certificated El 60 Fire Resistant.
Round or Squared Front Plate Available.

4.3.6 NARROW PROFILE MORTISE LOCK & STRIKE

EURO lock (axe distances 46mm.)
Euro lock is a mortise lock with latch projection which means the latch is automatically projected and deadlocked when the door is closed. This mortise lock is suitable for all kinds of wooden door whether it’s a hotel room, office or warehouse door etc. The latch projection function increases security by making it impossible to gain access by using plastic cards.
For additional security the option to order this lock with a deadbolt shall be available.

The Wide Profile Mortise Lock & Strike shall comply with the following specifications:

- Lock Case, Latch and Deadbolt made of Steel;
- Axes Distances : 46mm;
- 8mm Square Spindle;
- Turning Angle 30º;
- Different Backsets;
- Available CAM Cylinder Profiles :
  - Euro Profile;
  - UK Oval Profile;
- Available Finishes :
  - Satin Stainless Steel;
  - Gold Enamelled.
- Reversible Latch and Auxiliary Latch (Anticard).
- With Auxiliary Latch (Anticard) it Deadlocks the Latch.
- Handle Retracts the Latch to Normal Position.
- Panic Function Option (Handle Retracts the Latch and the Deadbolt).
- Deadbolt Detector Option for Electronic Privacy Function.
- Mortise Lock EN 12209 Grade 3 (High Frequency of Use or With Care, Use in Public Buildings).
- Mortise Lock EN179 Grade 3* (Suitable for Use in Busy, High Traffic Areas).
- EN-1634-1 Certificated El 60 Fire Resistant.
- Round or Squared Front Plate Available.

4.4 SEMI-ONLINE (WIRELESS) COMPONENTS

The Semi-Online (Wireless) Solution should Deliver Real-Time High Level Security with all the Convenience of Battery Operated Access Control.
This Application is for a System with Low Power Consumption, providing Semi-Online Control without any need to Hard Wire the Door.
Should be Easy to Install by Setting-Up the Gateways (which should be Connected by Ethernet/WIFI or RS-485 to the Controlling PC) and Nodes in Pre-Defined Wireless Zones. The Battery Powered SAC Devices should be Configured Automatically through their Self-Organizing Capabilities and then use Built-In Low Power (2.4 GHz) Radio Transceivers to Communicate with The Gateways and Nodes to Create a Real-Time Semi-Online (Wireless) Access Control Network.

If a SAC Device should lose RF Connection at Any Time, it must Automatically Scan for a New Connection to an Alternative Gateway or Repeater, Restoring Communication and Maintaining Security.

In Case of Loss of Communication between the SAC Device and the Gateway or Repeater, the Wireless Standalone Lock should Automatically Switch to a Standalone Mode with VN Capabilities, and Allow or Deny the User from Accessing.

**4.4.1 POE GATEWAY**

The Gateway is the Link between the Network and Wirelessly Connected SACs (Wireless SACs). It shall give Real-Time Information to the Software. Gateways are Completely Managed through the Access Control Software, as they collect all the Information sent by the SACs and the Nodes that belong to that Gateway. It has been designed with PoE technology, capable of powering the Gateway through Ethernet infrastructure.

**The PoE Gateway shall comply with the following specifications :**

WPAN :
- Wireless Radio Frequency based on IEEE 802.15.4 at 2.4 GHz.
- Power Supply : PoE;
- Encryption :
  - AES 128bits encryption.
- Connection to the Network via RJ45 Ethernet;
- Shall be Able to Manage up to 6 Nodes and 16 Locks;
- Maximum of 112 Locks through the Gateway and Node Channel;
- Firmware Update via Software through Ethernet Connection;
- Tamper Switch.
4.4.2 RS-485 GATEWAY

The Gateway is the Link between the Access Controller and Wirelessly Connected SACs (Wireless SACs). It shall give Real-Time Information to the Software. Gateways are Completely Managed through the Access Control Software, as they collect all the Information sent by the SACs and the Nodes that belong to that Gateway. It has been designed with PoRS-485 technology, capable of powering the Gateway through RS-485 infrastructure.

The PoE Gateway shall comply with the following specifications:

- WPAN:
  - Wireless Radio Frequency based on IEEE 802.15.4 at 2.4 GHz.
  - Power Supply: PoRS-485;
  - Encryption:
    - AES 128bits encryption.
- Connection to the Access Controller via RS-485;
- Shall be Able to Manage up to 6 Nodes and 16 Locks;
- Maximum of 112 Locks through the Gateway and Node Channel;
- Firmware Update via Software through Ethernet Connection;
- Tamper Switch.

4.4.3 RS-485 NODES:

The Node is a Bridge between the Gateway and other Nodes or SACs, where the distance to the SACs or where the number of SACs that must be linked to the Gateway exceeds what is possible with a Single Gateway.

The RS-485 Node shall comply with the following specifications:

- WPAN:
  - Wireless Radio Frequency based on IEEE 802.15.4 at 2.4 GHz.
  - Power Supply: PoRS-485;
  - Encryption:
    - AES 128bits encryption.
- Connection to the Gateway via RS-485;
- Maximum of 6 Nodes per Gateway;
- Each Node shall Handle up to 16 Wireless SACs;
- Firmware Update via the Gateway;
- Tamper Switch.

COPYRIGHT – This document shall not be used or reproduced without the prior authorisation of Secelec ©
Tenderers to note that a number of Sallis (by SALTO) RS-485 Nodes have already been pro-cured though the building contracts, integration to these RS-485 Nodes is mandatory.

4.5 ONLINE ACCESS CONTROL

It is a composed of a hard wired Door Controllers located in a the Data Hub Rooms or IT Server Rooms connected to either hardwired Card Readers for a full Online Solution or Gateways and Nodes for a Semi-Online Solution or a combined solution.

4.5.1 DOOR CONTROLLER

The Door Controller is an Online Door Controller that can have multiple Card Readers connected and has Virtual Network (VN) capabilities.

Cards are automatically updated with the latest changes in the Access Plan, it records the User Audit into the Software and provides Advanced Information on Battery Status.

It also continually updates the Cancelled ID Carrier Black List Simply by Using the Cards on the Network, Distributing the latest Access Information throughout the Building via the Offline Standalone Locks.

Access Control changes can be Carried Out on the Software and these are then Actioned at the Door Controller in Real Time. It provides Full Online features via the Networked Live Link such as Door Monitoring Status, Remotely Controlling Door Opening, Roll Call, Zone Lockdown, Limited Occupancy etc.

4.5.2 SERVER / DOOR CONTROLLER INTERFACE

The Access Control Server shall interface to the proposed Door Controllers and Operator Workstations on which the Physical Security Information Management(PSIM)/Security Management System (SMS) application is installed using a standard 100/1000 Ethernet LAN. The system can achieve this using Door Controllers with a direct Ethernet LAN connector (preferred) or an IP converter.

The server LAN adapter card shall communicate with Door Controllers by means of a TCP/IP protocol that provides error-free peer-to-peer data communication at rates of up to 1000Mbps. Systems that employ host/slave (polling) architecture from the server to the Door Controller shall not be acceptable.

The architecture of the networking system shall allow Door Controllers to be connected in a multi-dropped (daisy chain) fashion using standard UTP CAT-6 or Mylar 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 installer demonstrate the capability of the Server / Door Controller interface to support reliable data acquisition from Card / Biometric Readers, Card / Biometric Reader Controllers and Door Controllers while the system is operating at a load of 100,000 card Reader transactions per hour.

The functionality of the Server / Door Controller interface shall be accessible to any standard Windows Server 2012 or later, Windows 7 or Windows 8.1 compatible software application via drivers provided by the hardware vendor or installation contractor.
The Access Control System vendor shall also provide low level software tools that enable system integrators and administrators to monitor, diagnose and control all functionality provided by the network of IP Converters and Door Controllers. These software tools shall be accessible directly from any computer on the Server / Door Controller Network.

4.5.3 DOOR CONTROLLERS

4.5.3.1 DOOR CONTROLLER NETWORK

The use of networked Door Controllers shall facilitate the modular implementation of portions of the Access Control System as required by the client. This network may be either an RS-485 multidrop network or a TCP/IP socket interface on an Ethernet LAN. No other type of network infrastructure will be considered.

4.5.3.2 DOOR CONTROLLER FUNCTIONALITY AND PERFORMANCE

4.5.3.2.1 GENERAL

The door controller shall be a fully embedded unit and shall if required run a proven stable embedded operating system.

Door Controllers shall provide automatic switching between online and offline modes.

Online mode is defined as the mode in which Access Control decisions are made by the central Security Management System (SMS) Server.

Offline mode is defined as the mode in which Access Control decisions are made by the Door Controller based on locally stored system configuration and permissions data.

The Door Controller shall be capable of detecting a break in its communication link with the host computer. When such a break is detected, the Door Controller shall automatically switch to offline mode. In offline mode, the Door Controller shall continue to process requests for access received from Readers connected to the Door Controller. This includes request for Access from the Sallis (by SALTO) locks.

4.5.3.2.2 MEMORY

Where appropriate, the tenderer shall install Door Controllers equipped with as standard sufficient non-volatile memory to be capable of:

- Storing 250,000 card holders or biometric profiles in Offline mode.
- Storing 2,000,000 events in Offline mode.

4.5.3.2.3 POWER SUPPLY

The Door Controller shall have a separate monitored, battery backed, AC power supply. The power supply shall further be On-Board surge protected.
The surge protection shall as a minimum include all of the following components:

- Transzorps;
- Metal-Oxide Varistors (MOVs);
- Gas Arrestors.

Any system that requires additional surge protection or a separate PC board to achieve this level of protection will not be considered.

4.5.3.2.4 COMMUNICATIONS INTERFACE

All communications interfaces shall be On-Board optically isolated to at least 18 kV. Any system that requires additional isolation or a separate PC board to achieve this level of protection will not be considered.

Inputs and Outputs

The following I/O is required as a minimum:

- 8 X Opto-Isolated Digital Inputs;
- 8 X Digital Outputs of the Changeover Relay Contact Type.

A digital input shall be switched on when a voltage in the range 5 VDC – 60 VDC 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.

4.6 ACCESS CONTROL MANAGEMENT TOOLS

To Perform Routine Tasks such as Editing New User Keys, Set Up the Access Control Plan, Run Diagnostics on Offline and Semi-Online (Wireless) Devices, Perform Emergency Openings in Extreme Situations etc.

4.6.1 CARD ENCODER

The Card Encoder shall comply with the following specifications:

Main Functions:
- Encode Cards for Guests and Staff/Students;
- Verify the Encoding is Properly Made on the Cards;
- Read Information from the Cards;
- Update Cards.

Technical Data:
- The Encoder shall be a Compact Device which Reads, Encodes and Updates Cards.
- Should be Available in Different Versions depending on the PC connection (USB or Ethernet).
- It should Permit Automatic Key Issuing in Large Volumes and Initialize Doors.
4.6.2 PORTABLE PROGRAMMING DEVICE (PPD)

Main Functions:
- The PPD is the Messenger between the Software and the SACs.
- The PPD shall have a Multilingual Interface.
- Minimum of 6 Languages.
- ID technologies available: MIFARE DESfire, Vicinity, HID iClass.

Technical Data:
- Battery Powered:
  - 3 X Standard Alkaline Batteries - LR03 – AAA, 1.5 V;
- PC Connection: USB.
- Collect Audit Trails from Offline SACs;
- Update Locks (Door Profile & Internal Clock);
- Door Diagnostic;
- Emergency Opening;
- Firmware Update.

4.7 WARRANTY

Manufacturer’s Warranty: Provide written warranty, signed by manufacturer and Installer agreeing to replace Access Control System Devices and Equipment that fail in Materials or Workmanship within Specified Warranty Period.

Warranty Period: 24 month from date of Completion.
4.8 ADDITIONAL HARDWARE
4.8.1 CARD READER SPECIFICATION

Card readers shall be "single-package" type, combining controller, electronics and antenna in one package, in the following configurations:

Provide "single-gang" mounting style contactless smart card readers for wall mounting, vehicle stanchions and pedestals, and where shown on plans. It is allowable for the reader shall require that a card, once read, must be removed from the RF field for one second before it will be read again, to prevent multiple reads from a single card presentation and Anti-Passback errors. The reader shall have a lifetime warranty against defects in materials and workmanship. Colour shall be selected by the Architect. Standard colours shall include:
- Gray;
- Black;
- White.

4.8.1.1 CARD READER TYPE 1 – MIFARE / ISO 14443 / DESFIRE EV 1

The reader shall be used to read cards or tags from the Mifare® / ISO 14443 families.

The reader shall comply with the following specifications:

- Export the ID number of the Mifare® card.
  - Type 1 : ISO 14443A-2 (Mifare®) serial number reader [Communication speed 106K bit/s].
  - Type 2 : ISO 14443A-3 (Mifare®) read/write sector reader [Communication speed 106K bit/s].
  - Type 3 : ISO 14443A-4 DESFire reader [Communication speed 106K bit/s].
  - Type 4 : ISO 14443-4AB T=CL read/write reader [(T=CL) communication speed between chip and reader 848K bit/s (card and card-OS dependent.)].

- Input Voltage : 5 - 14VDC.
- Operating Current :
  - Average : 100mA.
  - Peak : 250mA.
- Processing Speed : less than 0.1 second.
- Reading Distance : 5 – 15cm.
- Operating Frequency : 13.56 MHz.
- Readers shall be fully potted ensuring that weather does not affect them when located outside (weather and vandal resistant).
- Minimum of an IP66 rating.
- Operating Temperature Range : -20 – +65°C.
- Relative Humidity : 0 – 95% Non-condensing Relative Humidity.
- Interfaces :
  - Wiegand 26 bit signal.
  - RS-485.
Certifications:
- Canada/UL 294 Listed.
- FCC Certification.
- Canada Certification.
- EU and CB Scheme.
- IEC60950 ITE Electrical.
- EN 300 330 – SRD.
- CE Mark.
- Australia C-Tick.
- Taiwan, China.
- ACA.
- CAC compliant.

Information encrypted and duplex verified.
Anti collision, read more than one card at the same time.
Approximate Wiegand signal communication distance: 70 meter.
Approximate RS-485 signal communication distance: 1200 meter.
The reader shall have either 1 X Bi-colour LED (red & green) or 2 X Single Colour LEDs (red & green) to indicate that a card has been read and access has been granted or denied.
The reader shall have a beeper or buzzer to give an audible indication of whether a card has been read.
Full 2 year warranty.
Fits on a standard 2x4 electrical box (or can be made to fit neatly).
Be mountable directly onto metal with no change in read range performance.
If readers are mounted back to back on a 30mm thick aluminium door or on a single drywall there shall be no reader interference, or the readers shall be screened to prevent reader interference.

Type 4: ISO 14443-4AB T=CL shall as a minimum requirement be capable of reading cards from the following manufacturers:

- Sharp.
- Infineon.
- ST.
- Atmel.

4.8.2 CARD READER INTERFACES

4.8.2.1 WIEGAND

Wiegand 26: The reader outputs the 24 least significant bits of the card number contained in the SEIWIG container plus two parity check bits.

The Wiegand 26 bit output format shall comply with the following specifications:

- Data Structure:
  - Bit 1 - Even Parity check bit for bit 2-13.
  - Bit 2-25 - Card Number Data.
  - Bit 26 - Odd Parity check bit for bit 14-25.

4.8.2.2 RS-485

RS-485: The reader outputs all 40 digits of the SEIWIG container.

The RS-485 serial output signal shall comply with the following specifications:
Output signal specification: Required compatible with whole system, client provides interface protocol.

4.8.3 ACCESS CARDS

Access cards shall be used with access card readers to gain entry to access controlled portals (e.g.; doors, gates, turnstiles) and to hold information specific to the user.

The card shall be available in single technology or multiple technology configurations.

A sample of the card with a card holder and lanyard shall be provided to the engineer for approval before the cards are ordered.

As a standard Single technology cards shall meet the following criteria:

The card shall meet the following card standards:

The card shall meet ISO 7810 specifications for length, width, thickness, flatness, card construction and durability, and shall be in a form suitable for direct two-sided dye-sublimation or thermal transfer printing on the specified badge printer.

Presentation to the access control reader at any angle within a minimum of one (1) inch shall result in an accurate reading of the card.

Unique 64-bit, fixed card serial number, used for anti-collision and key diversification.

The card shall support read/write capability, with a minimum of 2 Kbits [256 bytes] of EEPROM memory or 16 Kbits [2048 bytes] of EEPROM memory. The 2 Kbit card shall have a minimum of 2 Application Areas, and the 16Kbit shall have either (specify) 2 or 16 Application Areas to support future applications. Data retention shall be 10 years, nominal.

Wiegand card data up to 84 bits in length shall be factory programmed in Application Area 1 for use with access control systems.

Each Application Area on the card shall be secured with a 64-bit unique, diversified security key, such that data stored in that area cannot be accessed or modified until the card and reader have completed a mutual authentication process.

The card shall be capable of completing any write operation, even if the card is removed from the RF field during that operation.

The card shall be warranted against defects in materials and workmanship for two (2) years, or if multiple technologies are used: with a magnetic stripe the card shall have a fifteen (15) month warranty; or with a contact chip, the card shall have a one (1) year warranty.

Provide (specify quantity), “smart” access cards, compatible with the specified card readers. Cards shall be encoded with Wiegand card data, at the factory.

The card shall not carry any identification showing the location of the property unless otherwise specified herein.

The card shall be capable of accepting a slot punch on one end, allowing it to be hung from a strap/clip in a vertical orientation.
As a standard Multiple technology cards shall meet the following additional criteria:

The card shall support Mifare® / ISO 14443 contactless smart chip and antenna plus any or all of the following technologies, simultaneously:
- HID Proximity chip and antenna.
- EM Proximity chip and antenna.
- HITAG™ 1 Proximity chip and antenna.
- HITAG™ 2 Proximity chip and antenna.
- Magnetic Stripe.
- Embedded Contact Smart Chip Module.
- Barcode.

4.8.3.1 READ/WRITE ISO PROXIMITY MIFARE / ISO 14443 / DESFIRE EV 1 CARDS

Mifare® DESFire EV 1 series cards complying with the specifications as set out in Section 4.8.3.

4.8.4 BIOMETRIC READER SPECIFICATION

Biometrics will not be utilised in the system at this current time, apart from operator workstation control, but the system must be fully capable of upgrading to a Biometric System without the addition of any hardware or any firmware or software changes.

No capacitive type fingerprint readers will be accepted. The fingerprint reader shall operate on an optical fingerprint capturing system.

4.8.4.1 BIOMETRIC READER TYPE 1 – FINGERPRINT – PC ACCESS CONTROL AND TAKE-ONS

This biometric (fingerprint) reader shall be used to authenticate users on PC’s with highly sensitive information.

The Biometric Reader shall have the following minimum specifications:

- 1:1 Authentication and 1: Many Identification.
- Cryptographic security.
- An RS 232 or USB interface.
- A PC software for image capture, template processing, authentication and identification up to 1:20,000 persons.
- 500 DPI resolution @ 8 bit greyscale.
- A 20mm X 20mm or larger acquisition area.
- An operating temperature range of 0 °C to 40 °C or better.
- Less than 2,5W power consumption.
- Be able to operate on Windows 2000, 2003 and XP platforms. Verification time < 1.5s – Identification time < 2.5s (for a database of 3000 people).

4.8.4.2 BIOMETRIC READER TYPE 2 – FINGERPRINT WITHOUT A KEYPAD & LCD : INDOOR
This biometric (fingerprint) reader shall be used to authenticate users entering or leaving an area with highly sensitive information. The biometric reader shall be equipped with an alpha-numeric keypad for entering a "PIN" code as well as a LCD display for displaying user relevant information.

The Biometric Reader shall have the following minimum specifications:

1:1 Authentication & 1: Many Identification.
Local database management.
Standalone or networked operation.
500 DPI resolution finger scanner.
A 500 record or better internal user storage capacity.
A 5000 record or better internal transaction storage capacity.
Interfaces shall include all of the following:
- RS-485.
- Ethernet 10/100 Base T.
- Six optional I/O ports.
The unit shall be able to do fake finger detection.
An optional contact less card reader shall be available for the unit (Mifare A/B contact less proximity card reader compliant with ISO 14443).
Verification time < 1.5s – Identification time < 2.5s (for a database of 3000 people).
Compliance with: EN60950, EN55024, EN55022, FCC15, UL1950, CE Approval, UL 94, V0 material.
Power: 12 VDC / 30W.
Maximum Size: L: 145 mm H: 160mm D: 75 mm.
Environmental Specifications: 0°C TO +40°C @ 80% Non-Condensing Relative Humidity.

It shall further be possible to integrate a number of different proximity card readers into the biometric reader unit.

4.8.4.3 BIOMETRIC READER TYPE 3 – FINGERPRINT WITH KEYPAD & LCD: INDOOR

This biometric (fingerprint) reader shall be used to authenticate users entering or leaving an area with highly sensitive information. The biometric reader shall be equipped with an alpha-numeric keypad for entering a "PIN" code as well as a LCD display for displaying user relevant information.

The Biometric Reader shall have the following minimum specifications:

1:1 Authentication & 1: Many Identification.
Local database management.

Standalone or networked operation.
500 DPI resolution finger scanner.
A Backlit LCD graphical display.
A Backlit keypad with 12 keys (0 to 9, *, #) plus at least four programmable function keys.
A 500 record or better internal user storage capacity.
A 5000 record or better internal transaction storage capacity.
Interfaces shall include all of the following:
- RS-485.
- Ethernet 10/100 Base T.
Six optional I/O ports.
The unit shall be able to do fake finger detection.
An optional contact less card reader shall be available for the unit (Mifare A/B contact less proximity card reader compliant with ISO 14443).
Verification time < 1.5s – Identification time < 2.5s (for a database of 3000 people).
Compliance with: EN60950, EN55024, EN55022, FCC15, UL1950, CE Approval, UL 94, V0 material.
Power: 12 VDC / 30W.
Maximum Size: L: 145 mm H: 160mm D: 75 mm.
Environmental Specifications: 0°C TO +40°C @ 80% Non-Condensing Relative Humidity.

It shall further be possible to integrate a number of different proximity card readers into the biometric reader unit.

4.8.4.4 BIOMETRIC READER TYPE 4 – FINGERPRINT: OUTDOOR

This biometric (fingerprint) reader shall be used to authenticate users entering or leaving a building with highly sensitive information.

The Biometric Reader shall have the following minimum specifications:

1:1 Authentication & 1:Many Identification.
Local database management.
Standalone or networked operation.
500 DPI resolution finger scanner.
A Backlit LCD graphical display.
A Backlit keypad with 12 keys (0 to 9, *, #) plus at least four programmable function keys.
A 500 record or better internal user storage capacity.
A 5000 record or better internal transaction storage capacity.
Interfaces shall include all of the following:
- RS-485.
- Ethernet 10/100 Base T.
Six optional I/O ports.
The unit shall be able to do fake finger detection.
An optional contact less card reader shall be available for the unit (Mifare A/B contact less proximity card reader compliant with ISO 14443).
Verification time < 1.5s – Identification time < 2.5s (for a database of 3000 people).
Compliance with : EN60950, EN55024, EN55022, FCC15, UL1950, CE Approval, UL 94, V0 material.
Power: 12 VDC / 30W.
Maximum Size : 220mm X 300mm X 100 mm.
Environmental Specifications: -10°C TO +45°C @ 80% Non-Condensing Relative Humidity.
Weatherized for outdoor use. Visor protects display and sensor. Use of the Error! Reference source not found. is required.

It shall further be possible to integrate a number of different proximity card reader into the biometric reader unit.

4.8.5 BREAKGLASS SPECIFICATION
4.8.5.1 BREAKGLASS TYPE 1 – ACCESS CONTROL : GREEN

The break glass shall have the following specifications :

- The break glass shall be able to switch 50VAC or 30 VDC @ 8A.
- The break glass shall be able to switch 50VDC @ 3A.

Environmental Conditions :
- Temperature Range : -40°C – +85°C.
- Relative Humidity : 0 – 90% Non-Condensing Relative Humidity.

The break glass shall be operable with a glass lens or a resettable lens.
The break glass shall have surface and flush mounting options.
The break glass shall have a high quality micro switch.
The break glass shall have the standard EN54 symbols on it.
Accept hinged cover as a standard.
The break glass shall have a built in key test facility.

Breakglass units shall be in accordance with BS 5839-2.
The unit shall be large enough to cover 65 mm ø conduit draw box when the unit is surface mounted.
Flush mounted units shall be provided with a special flush mounting box, which can accept electrical conduit terminations.
Surface mounted units shall be deep enough to terminate 20 mm ø conduits into the unit, and shall be mounted solidly on the wall by means of their back plates.
The wiring terminals of the unit shall be able to accept wiring lugs, and shall be of the screw and clamp plate type to hold a lug firmly pressed against its contact surface. Spring loaded push-in contacts will not be acceptable.
4.8.5.2 BREAK GLASS LENSES – RESETTABLE PLASTIC

The Resettable Break Glass Lens shall have the following specifications:

- The glass shall not be damaged when it is pressed.
- The glass shall be resettable with a standard break glass key.
- The glass shall be marked with the standard EN54 symbols and/or a "PRESS HERE" indication.

4.8.6 SOUNDERS

4.8.6.1 TYPE 1 - MINI SOUND BOMB

This sound bomb is for internal use only and is normally mounted in the hallway of a building.

The Mini Sound Bomb shall comply with the following specifications:

- Sound Projection Level (SPL) [dB/1m] : 105 dB ±3 dB.
- Maximum Current Consumption : 300 mA.
- Operating Voltage :
  - Nominal : 12 VDC.
  - Range : 9 – 14 VDC.
- Environmental Conditions :
  - Temperature Range : -40°C – +85°C.
  - Relative Humidity : 0 – 90% Non-Condensing Relative Humidity.
  - Minimum IP Rating : IP32.

4.8.6.2 TYPE 2 – SIREN

The siren type sounder is for external use mounted at roof level at eave ceiling or under roof overhang.

The Multi-Tone Siren shall comply with the following specifications:

- Sound Projection Level (SPL) [dB/1m] : 110 dB ±3 dB.
- Maximum Current Consumption : 600 mA.
- Operating Voltage :
  - Nominal : 12 VDC.
  - Range : 9 – 14 VDC.
- Environmental Conditions :
  - Temperature Range : -40°C – +85°C.
• Relative Humidity : 0 – 95% Non-Condensing Relative Humidity.
• Minimum IP Rating : IP67.
The siren shall have selectable tones.

4.8.7 KEY OVERRIDE SPECIFICATION

4.8.7.1 KEY-OVERRIDE – HIGH SECURITY

High security key-override shall comply with the following specifications:

Three (3) high security keys, with key certificates.
Electrical Contacts:
Double Change-Over Contact.
Minimum Contact Rating : 100V @ 0.5A.
Mounting Accessories.

4.8.8 DOOR POSITION SWITCHES SPECIFICATION

4.8.8.1 TYPE 1 – FLUSH MOUNT

This type is used in aluminium, steel or wooden doors for monitoring the door status.

The DPS shall comply with the following specifications:

Operating gap (minimum) 10 mm.
Connection via 4 wires.
Contact type must be NC or NO.
Typical Dimensions Ø22 x 40 mm to Ø26 x 40 mm.
Colour:
White;
Beige;
Brown.
Minimum Contact switching rating : 100V @ 0.5A.
Environmental Conditions:
• Operating Temperature Range : -40 – +65º C.
• Relative Humidity : 5 – 95 % Non-Condensing.
5 WIRELESS INTRUDER DETECTION HARDWARE

5.1 GENERAL

Intruder Detection (Alarm) Systems will be installed in all areas with windows on the ground and first floors. The locations will be indicated on the Engineers Drawings.

The system will be a Wireless Intruder Detection System to facilitate the easy movement/addition/removal of detectors without the need to rewire portions of the building. The buildings will be saturated with sufficient wireless receivers to enable this.

The system will be fully integrated to the Access Control System and a user exiting the building after locking his/her office will activate the PID (Passive Infra-Red Detector) in his/her office.

5.2 INTRUDER DETECTION MANAGEMENT SYSTEM

5.2.1 SCOPE

This specification covers the general technical specifications and components of Intrusion Detection Management System (IDMS).

5.2.2 GENERAL REQUIREMENTS

The Intrusion Detection Management System will provide advanced, seamless integration with any Intrusion Detection Panel, provided they satisfy the requirements.

The IDMS will allow the CLIENT to monitor intrusion detection alarms inside the SYSTEM Alarm Monitoring module, in addition to giving the CLIENT command and control of supported intrusion detection devices (such as arming and disarming an area).

Once alarms are brought into the SYSTEM, they will be linked to digital video, global I/O activity will be triggered, and they will be stored in the SYSTEM audit trail. In addition, System Operators will monitor the status of intrusion detection devices from the SYSTEM Alarm Monitoring workstation (Control room).

The SYSTEM will not be the mechanism for initial configuration and setup of Intrusion Detection Devices and basic intrusion detection functionality. All IDMS configuration listed below will be for used for integration functionality within the SYSTEM.

5.2.3 SYSTEM OPERATION

5.2.3.1 INTRUSION DETECTION PANELS

The IDMS will allow for the configuration of an Intrusion Detection Panel.

Each Intrusion Detection Panel will be given a user defined name for up to 32 characters. A workstation name will be assigned to the intrusion detection panel.

System Administrators will have the ability to mark Intrusion Detection Panels as 'on-line' or 'off-line' depending on the state of the panels.

The intrusion detection panel’s communication will be either Ethernet (Preferably), Wireless, RS-485 or RS-232.

When a panel is added, On-Board devices (zones, relays) will be defined and added to the SYSTEM database.

5.2.3.2 INTRUSION DETECTION ZONES

The IDMS will allow for the configuration of Intrusion Detection Zones.

Each Intrusion Detection Zone will be given a user defined name for up to 64 characters.
System Administrators will have the ability to mark intrusion detection zones as ‘enabled’ or ‘disabled’. System Administrators will have the ability to mark intrusion detection zones as output zones (Detection Systems Only).

5.2.3.3 INTRUSION DETECTION AREAS

The IDMS will allow for the configuration of Intrusion Detection Areas. Each Intrusion Detection Area will be given a user defined name for up to 64 characters. System Administrators will have the ability to mark intrusion detection areas as ‘enabled’ or ‘disabled’.

5.2.3.4 INTRUSION DETECTION PANEL USERS

The IDMS will allow for the configuration of Intrusion Detection Panel Users. A Panel User will be able to be linked to a SYSTEM cardholder record.

5.2.3.5 INTRUSION DETECTION ON-BOARD RELAYS

The IDMS will allow for the configuration of Intrusion Detection On-Board Relays. Each Intrusion Detection On-Board Relay will be given a user defined name for up to 64 characters. System Administrators will have the ability to mark intrusion detection On-Board Relays as ‘enabled’ or ‘disabled’.

5.2.3.6 INTRUSION DETECTION OFF-BOARD RELAYS

The IDMS will allow for the configuration of Intrusion Detection Off-Board Relays. Each Intrusion Detection Off-Board Relay will be given a user defined name for up to 64 characters. System Administrators will have the ability to mark intrusion detection Off-Board Relays as ‘enabled’ or ‘disabled’.

5.2.3.7 INTRUSION DETECTION DOORS

The IDMS will allow for the configuration of Intrusion Detection Doors. Doors will be able to be configured for each panel. Each Intrusion Detection door will be given a user defined name for up to 64 characters. System Administrators will have the ability to mark intrusion detection doors as ‘enabled’ or ‘disabled’.

5.2.4 ALARM MONITORING INTEGRATION

5.2.4.1 GENERAL ALARM MONITORING INTEGRATION

The SYSTEM will allow for annunciation of intrusion detection alarms in the Main Alarm Monitoring Window. Intrusion Detection alarms reporting into the Main Alarm Monitoring Window will report just like any other access control alarm and will have the same annunciation and display properties as access control alarms.
5.2.4.2 ALARM VIEW

Alarms from the Intrusion Detection panel will be displayed in the Main Alarm Monitoring Window. In the Alarm View, the following columns will be utilized:

- **Alarm Description**
- **Time/Date**
- **Controller** - will display the name of the Controller
- **Device** - will display the name of the Device (zones, On-Board relay, Off-Board Relay, door)
- **Card** - will display the name of the linked SYSTEM cardholder
- **Alarm Priority**
- **Text** - will indicate whether there is additional text associated with the alarm
- **Intrusion Area** - will indicate the name of the area associated with the alarm.

5.2.4.3 ALARM DETAILS

The SYSTEM will support an Alarm Details description that will show the ‘Alarm Description’, ‘Time/date’, ‘Controller’, ‘Device’, and ‘Area’ associated with the alarm. The information will also display the linked SYSTEM user.

5.2.4.4 SYSTEM HARDWARE STATUS TREE

Intrusion Detection devices and areas (Controllers, Zones, On-Board Relays, Off-Board Relays, doors) and areas will be displayed in the System Hardware Status Tree.

5.2.4.5 INTRUSION DETECTION TRACING

The IDMS will support tracing of intrusion detection devices and areas.

5.2.4.6 REAL TIME STATUS INDICATORS AND INFORMATION

The SYSTEM will be able to report status information for the Intrusion Detection Devices. The following Status Information for Intrusion Detection Panels will be able to be displayed:

- Firmware Version
- Online status
- Internal Event Log Threshold Reached
- Internal Event Log Wrapped
- Point Bus Failed since it Last Reported
- Valid Local Access
- RF Receiver Trouble
- Failed to Call RAM
- User Code Tamper
- SDI Device is Failed
- Receiver Communications Has Failed
- AC Failure
- Battery is Missing
- Battery is Low
- Parameter Checksum Failed
- Phone Line Failed
- Extra RF point
- Report Failure
- Control Fault
- MPX Bus Fault
- Radio RX Fault
- AUX Power Fault
- Option Fault
The status for the intrusion detection zones will be displayed in Alarm Monitoring:
- Bypassed / Un-bypassed
- Forced / Not Forced
- Normal, Shorted, Open, Missing (Not Responding), Not Defined (Not Programmed)
- Unacknowledged / Acknowledged
- Explicit Trouble
- Tamper
- Low Battery [Radio Zone]
- No Signal Strength [Radio Zone]
- Alarm (un-restored)
- Trouble (un-restored)
- Untested
- Day Monitor Alarm
- Output Latched
- Short Circuit Fault
- Open Circuit Fault
- Low Resistance
- High Resistance
- RF Lid Tamper – only RF zones
- RF Supervision Fail – only RF zones
- RF Low Battery – only RF zones
- RF Zone Fob Deleted – only RF zones
- If the zone is RF or normal
- Suspended

The status for the intrusion detection areas will be displayed in Alarm Monitoring:
- **Arm/Disarm Status:**
  - Disarmed
  - Not In Use
  - Entire Partition Armed
  - Perimeter Armed
  - Master Armed
  - Perimeter Instant Armed
  - Perimeter Delay
  - Area Entry Delay
  - Perimeter Entry Delay
  - Area Exit Delay
  - Perimeter Exit Delay
  - Master Armed Instant
  - Setting
  - Suspend
  - Partial Arm
- **Additional Area Status:**
  - Not Ready To Arm
  - Area Points Bypassed
  - Area Forced Points
  - Alarm Status
  - System
  - PA Alarm
  - Tamper Alarm

The status for the intrusion detection On-Board Relays will be displayed in Alarm Monitoring:
- **On / Off**

The status for the intrusion detection Off-Board Relays will be displayed in Alarm Monitoring:
- **On / Off**

The status for the intrusion detection doors will be displayed in Alarm Monitoring:
- **Door Mode:**
  - Unlocked / Locked
5.2.5 COMMAND AND CONTROL FUNCTIONALITY

5.2.5.1 INTRUSION PANEL COMMANDS

A command will be available to set the date and time on the intrusion panel. A command will also be available to read the date and time on the panel.

5.2.5.2 ZONE COMMANDS

A command will be available to bypass a zone. A command will also be available to un-bypass a zone. A command will be available to turn a zone output on. A command will also be available to turn a zone output off.

5.2.5.3 AREA COMMANDS

A command will be available to arm an area. The possible parameters include:
- Perimeter Arm – Arms the perimeter of the area.
- Arm Entire Partition – Arms both the interior and perimeter of the area.
- Master Arm Delay – Master (both perimeter and interior) arms (with exit and entry delays) the area.
- Master Arm Instant – Master (both perimeter and interior) arms (no delays) the area.
- Perimeter Delay Arm – Delay arms all perimeter points in the area.
- Perimeter Arm Instant – Instantly arms all perimeter points (no delays) in the area.
- Partial Arm – Partially arms the area, this means that only the zones that have been configured for partial arming will be armed with this command.
- A command will be available to disarm an area. A command will be available to silence alarms. A command will be available to Cancel/Reset alarms that have occurred for an area.

5.2.5.4 ON-BOARD RELAY COMMANDS

A command will be available to activate a relay output. A command will also be available to deactivate a relay output.

5.2.5.5 OFF-BOARD RELAY COMMANDS

A command will be available to activate an Off-Board Relay output. A command will also be available to deactivate an Off-Board Relay output.
A command will be available to toggle an Off-Board Relay output.
5.2.6 SYSTEM EVENTS

It will be possible to display events that have occurred on the IDMS panel as well as report any incoming events that occur on the panel while the panel is online. The list of available events for each panel is listed below:

- Access Granted;
- Duress;
- User Alarm;
- Bypass Point;
- Forced Point;
- Alarm;
- Trouble;
- Restore from Trouble;
- Missing Alarms;
- Missing Troubles;
- Point Opening;
- Point Closing;
- Extra Point;
- Point Bus Fail;
- All Points Tested;
- Restore from Alarm;
- User Code Added;
- Service Start;
- Sensor Reset;
- Relay Set;
- Relay Reset;
- Force Arm;
- Create Status Report;
- Walk Test Start;
- Walk Test End;
- Fail Open;
- Fail Close;
- Area Watch;
- Walk Test Point;
- Extend Close Time;
- Opening;
- Forced Close;
- Closing;
- Test Report;
- Log Threshold;
- Log Overflow;
- Parameter Change;
- User Code Tamper;
- User Code Change;
- Schedule Execute;
- Schedule Change;
- Date Change;
- Time Change;
- User Level Set;
- Valid Access;
- Invalid Access;
- Valid Remote;
- Invalid Remote;
- Communications Fail;
- Communications Restore;
- Phone Fail;
• Phone Restore;
• SDI Device Fail;
• SDI Device Restore;
• AC Fail;
• AC Restore;
• Battery Missing;
• Battery Low;
• Battery Restore;
• Watch Dog Reset;
• Supervision (non-fire);
• Remote Reset;
• Checksum Fail;
• Memory Fail;
• Re-Boot;
• Parameter Checksum Fail;
• Force Perimeter Instant;
• Force Perimeter Delay;
• Perimeter Instant;
• Perimeter Delay;
• Delete User;
• Point Bus Restore;
• RF Battery Low;
• RF Battery Restore;
• RF Tamper Restore;
• RF Receiver Trouble;
• RF Extra Point;
• RF Receiver Restore From Trouble;
• RF Interference;
• RF Tamper Alarm;
• RF Tamper Trouble;
• Equipment Restore;
• Door Secured;
• No Entry (Access Denied);
• Door Left Open;
• Network Fail;
• Network Restore;
• Network Condition;
• Equipment Fail;
• Extra Account;
• Low Signal Strength;
• RF Receiver Tamper;
• RF Receiver Restore from Tamper;
• RF Interference Restore
• Sensor Trouble;
• Sensor Trouble Restore;
• Door Locked;
• Fail to Execute;
• Analog Service;
• Analog Restore;
• Test Failed;
• External Device;
• Custom Function Executed;
• Unverified Event;
• Abort;
• Service Request;
• Output State;
- Output State Restore;
- Bypass Restore;
- Alarm Silenced;
- Alarm Panel Substitution;
- Burglary Alarm;
- Keypad Emergency;
- Keypad Panic;
- Open;
- Close;
- Bypass (24Hr, Supervisory);
- Bypass (Forced or When Closed);
- Un-bypass (24Hr, Supervisory);
- Trouble (Zone);
- Restore (Zone);
- Trouble (System);
- Restore (System);
- User Code Change;
- Time Change;
- Date Change;
- Access Code Used;
- Auto Arming Time Change;
- Remote Programming Access;
- Local Programming Access;
- Supervisory;
- Temporary Code Expiration Date Change;
- Communications Lost;
- Communications Restored;
- Access Granted;
- Access Denied;
- Holdup Alarm;
- Holdup Bypass;
- Holdup Restore;
- Holdup Trouble;
- Holdup Trouble Restore;
- Holdup Un-bypass;
- AC Restore;
- Access Lockout;
- Access Trouble;
- Automatic Test;
- Communications Fail;
- Communications Restore;
- Disarm From Alarm;
- Local Program;
- Local Programming Ended;
- Log Threshold;
- Manual Test;
- Parameter Checksum Fail;
- Phone Line Restore;
- Phone Line Trouble;
- Power Up;
- Printer Online;
- Remote Program Begin;
- Remote Program Denied;
- Remote Program Success;
- Schedule Executed;
- System Power Restore;
5.2.7 STATUS REQUIREMENTS

The following list of status reporting will be included for SYSTEM integration, specific to each panel:
- Zone Active;
- Zone Short;
- Zone Open;
- Zone In Explicit Trouble;
- Zone Tamper;
- Zone Not Responding;
- Zone Low Battery;
- Zone No Signal Strength;
- Zone Not Programmed;

• System Battery Trouble;
• Test End;
• Test Report;
• Test Start;
• Time Changed;
• Transmitter Battery Restore;
• Transmitter Battery Trouble;
• User Code Tamper;
• Door Forced;
• Door Forced Trouble;
• Emergency Alarm;
• Emergency Bypass;
• Emergency Restore;
• Emergency Trouble;
• Emergency Trouble Restore;
• Emergency Un-bypass;
• Expansion Restore;
• Expansion Trouble;
• Panic Alarm;
• Panic Bypass;
• Panic Restore;
• Panic Trouble;
• Panic Trouble Restore;
• Panic Un-bypass;
• RF Interference;
• RF Interference Restore;
• Tamper Alarm;
• Tamper Bypass;
• Tamper Restore;
• Tamper Un-bypass;
• Un-typed Zone Trouble;
• Burglary Alarm;
• Burglary Bypass;
• Burglary Cancel;
• Burglary Restore;
• Burglary Test;
• Burglary Trouble;
• Burglary Trouble Restore;
• Burglary Un-bypass;
• Burglary Verified;
• Relay Close;
• Relay Open.
• Zone Bypassed;
• Zone Force Bypassed;
• Zone In Alarm;
• Zone In Trouble;
• Zone Untested;
• Zone Day Monitor Alarm;
• Zone Output Latched;
• Firmware Revision Listing;
• Panel Time;
• Status of All Incoming Events Generated at the Panel;
• Alarm Output State;
• Programmable Output State;
• Octal Relay Module State for All Relays;
• Arming State for All Areas;
• Keypad, Emergency, Medical;
• Burglar Zone Alarm;
• Supervisory;
• Burglar Zone Trouble;
• Open;
• Close;
• Forced Bypass;
• Bypass;
• Zone Restore;
• Zone Trouble Restore;
• Point Status;
• Unacknowledged Alarm Point Status;
• Off-Board Relay Status;
• Unacknowledged Supervised Point Status;
• Forced Point Status;
• Unacknowledged Trouble Point Status;
• Bypassed Points;
• Panel Status;
• Area Status;
• Door Status;
• Point Text;
• Firmware Revision;
• Point Condition;
• On Board Relay Status;
• User Induced Area Status Transitions;
• Alarm Status for Areas;
• Area Points Not Ready to Arm;
• Area Points Bypassed;
• Area Points Forced;
• Get Panel Time.

• **Panel Status:**
  • Online / Offline Status of the Controller;
  • Firmware Revision of the Controller.

• **Zone Status:**
  • Whether the Zone is Normal or RF;
  • Open;
  • Short Circuit Fault;
  • Open Circuit Fault;
  • Low Resistance;
  • High Resistance;
  • RF Lid Tamper (only applicable to RF zones);
  • RF Supervision Fail (only applicable to RF zones);
5.2.8 PANIC PUSH BUTTON ALARM SYSTEM
5.2.8.1 ACTIVATION

Activation of any push button shall sound an audible tone in the associated control room and cause the associated icon on the operator control console to flash. The audible tone may be silenced from the control console causing the icon to remain steady with a red colour. The emergency condition of the icon shall only be reset once the latched button has been reset with the key release. All panic condition are time and date stamped and logged within the management workstation together with the current operator detail.

5.3 INTRUDER DETECTION SYSTEM COMPONENTS
5.3.1 CONTROL PANEL

The Control Panel shall be “heart” of the Intruder Detection System and shall have RS-485 Communications Busses (IDS-Busses) to expand the system and connect all required components be they wired or wireless.

The Control Panel shall comply with the following specifications:

Supply Characteristics:
- Nominal Voltage: 12 VDC;
- Voltage Range: 9 VDC – 16 VDC;
• Maximum Consumption:
  ▪ Standby – 100 mA;
  ▪ Alarm – 1.7 A.
• The DC Input shall be Fused.

Communication:
• **Protocol (IDS_Bus):**
  ▪ RS-485.
• Number of Ports:
  ▪ Outgoing: 2.
• Minimum Communications Range:
  ▪ 900 m.
• All Communications Busses shall be Opto-Isolated to Provide Protection from High-Voltage Spikes;

Operating Environmental Conditions:
• Temperature Range: -10°C – 70°C;
• Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
• Minimum IP Rating: IP40.

Indication:
• 3-LED Module Status Display:
  ▪ PC;
  ▪ Panel
  ▪ RX/TX Status.
• 8-LED Zone Status Display.

Inputs & Outputs:
• Inputs:
  ▪ 8 Hard Wired Zones (16 with Zone Doubling).
  ▪ 2-Wire Smoke Input;
• Selectable Input Resistors for:
  ▪ EOL;
  ▪ Tamper.
• Outputs:
  ▪ Supervised Bell Output;
  ▪ Auxiliary Output;
  ▪ Telephone Line.

Mounting Options:
• Wall Mounting.

Enclosure:
• Colour:
  ▪ RAL9011, black;
  ▪ RAL9003, white;
  ▪ More colours should be available on request of the Client.

Typical Dimensions:
• 280 mm x 280 mm x 75 mm Zinc Passivated Powder Coated Metal Box.

Certifications:
• Security Grade:
  ▪ EN 50131 – Grade 3;
• Environmental Grade:
  ▪ EN 50130-5 – Class II;
• Alarm Transmission Systems:
  ▪ EN 50136 – ATS 2;
• EMC Directive:
  ▪ EN 61000-6-3:2007/A1:2011;
  ▪ EN 50130-4:2011;
• Low Voltage Directive:
  ▪ EN 60950-1:2006/A12:2011;
• RTTE Directive:
- EN 60950-1:2006/A12:2011 – 3(1)(a)
- EN 45011 System 5:
- EN50131-1:2006+A1;
- EN50131-3:2009;
- EN50136-1-1:1998+A1,A2;
- EN50136-2-1:1998+A1;

Features:
- **IDS-Bus:**
  - RS-485.
  - Built-In Access Control Features
- **Shall Support:**
  - IP Module;
  - GPRS Module;
  - GSM Module;
  - Voice Module with Opto-Coupler Dialer Circuit.

**In-Field Firmware Upgrade via:**
- USB;
- Ethernet.

Automatic Daylight Savings Time feature;
Built-In Real-Time Clock with Backup Battery;
Programming of Remote Controls shall be possible using:
- Master Code;
- Or Installer Codes.

**Push Buttons:**
- Software Reset (Reset to Default Values and Restart);
- To Activate or Deactivate the Auxiliary Output.

The Control Panels in this series shall share the same programming for easy panel substitution.

Mean Time Between Failures (MTBF) : 50,000 Hours.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Maximum</th>
<th>On-Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Zones</td>
<td>192</td>
<td>8</td>
</tr>
<tr>
<td>PGMs</td>
<td>250</td>
<td>5</td>
</tr>
<tr>
<td>Multibus</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User Codes</td>
<td>999</td>
<td></td>
</tr>
<tr>
<td>Partitions</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Events Buffered</td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td>Expansion Modules</td>
<td>254</td>
<td></td>
</tr>
<tr>
<td>Remote Controls</td>
<td>999</td>
<td></td>
</tr>
</tbody>
</table>
5.3.2 CONTROL PANEL EXPANSION MODULES

5.3.2.1 8-ZONE HARDWIRED EXPANSION MODULE

The 8-Zone Hardwired Expansion Module shall be used to expand the number of hard wired zones available on the Intruder Detection System and shall connect via the IDS-Bus.

The 8-Zone Hardwired Expansion Module shall comply with the following:

Supply Characteristics:
- Bus Powered from the Control Panel:
- Nominal Voltage: 12 VDC;
- Voltage Range: 9 VDC – 16 VDC.
- Maximum Consumption:
  - Standby – 10 mA;
  - Alarm – 30 mA.
- The DC Input shall be Fused.

Communication:
- Protocol (IDS_Bus):
  - RS-485.
- Number of Ports:
  - Incoming: 1;
- All Communications Busses shall be Opto-Isolated to Provide Protection from High-Voltage Spikes;

Operating Environmental Conditions:
- Temperature Range: 0°C – 55°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
- Minimum IP Rating: IP54.

Indication:
- 3-LED Module Status Display:
  - PC;
  - Panel
  - RX/TX Status.
- 8-LED Zone Status Display.

Inputs & Outputs:
- Inputs: 8 Hard Wired Zones.

Mounting Options and Terminals:
- 35mm DIN Rail Mounting;
- Removable Terminals for Fast, Secure, Orderly and Economic Installations;

Enclosure:
- Colour: RAL9003, white;

Certifications:
- Security Grade:
  - EN 50131 – Grade 3;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
- EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;

Features:
- Connects Directly to the IDS-Bus;
- In-Field Firmware Upgradeable via IDS-Bus;
Each Output shall be Labelled for Easy Identification.
Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.2.2 32-ZONE WIRELESS EXPANSION MODULE

The 32-Zone Wireless Expansion Module shall be used to expand the number of hard wired zones available on the Intruder Detection System and shall connect via the IDS-Bus.

The 32-Zone Wireless Expansion Module shall comply with the following:

Supply Characteristics:
- Bus Powered from the Control Panel:
- Nominal Voltage : 12 VDC;
- Voltage Range : 9 VDC – 16 VDC.
- Maximum Consumption:
  - Standby – 10 mA;
  - Alarm – 140 mA.
- The DC Input shall be Fused.

Communication:
- **IDS_Bus Protocol**:
  - RS-485.
- Number of Ports:
  - Incoming : 1;
- All Communications Busses shall be Opto-Isolated to Provide Protection from High-Voltage Spikes;
- **Wireless Protocol**:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.

Operating Environmental Conditions:
- Temperature Range : 0°C – 55°C;
- Relative Humidity : 5% – 90% Non-condensing Relative Humidity;
- Minimum IP Rating : IP54.

Indication:
- 3-LED Module Status Display:
- PC;
- Panel
- RX/TX Status.
- 32-LED Zone Status Display.
Inputs & Outputs:
- Inputs:
  - 32 x Wireless Zones;
- Wireless Remotes:
- Minimum of 999;
- Wireless Programmable Outputs:
- Minimum of 8;
- Outputs:
  - 3 x Programmable Outputs;
  - 1 x Optional Output.
Mounting Options and Terminals:
- Wall Mounting;
Removable Terminals for Fast, Secure, Orderly and Economic Installations;
Enclosure:
- Colour: RAL9003, white;
Certifications:
- Security Grade:
  - EN 50131 – Grade 3;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
  - RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
- EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
Mean Time Between Failures (MTBF) : 50,000 Hours.

Features:
- Connects Directly to the IDS-Bus;
- In-Field Firmware Upgradeable via USB;
- Each Output shall be Labelled for Easy Identification.
Supervision:
- RF jamming
- Low Battery;
- Tamper;
- Check-In.
The RF Transmitter shall be capable of Displaying the RF Signal Strength of all Connected Devices;
The RF Transmitter shall be capable of doing a Noise Level Test and Indicating the Noise Levels of all Connected Devices;
Mean Time Between Failures (MTBF) : 50,000 Hours.
5.3.2.3 2-PORT HUB AND BUS ISOLATOR

The 2-Port Hub and Bus Isolator shall split and boost the signal on the Intruder Detection System RS-485 Communications Bus.

The 2-Port Hub and Bus Isolator shall comply with the following specifications:

Supply Characteristics:
- Bus Powered from the Control Panel:
- Nominal Voltage: 12 VDC;
- Voltage Range: 9 VDC – 16 VDC.
- Maximum Consumption:
  - Standby – 25 mA;
  - Alarm – 50 mA.
- The DC Input shall be Fused.

Communication:
- Protocol (IDS_Bus):
  - RS-485.
- Number of Ports:
  - Incoming: 1;
  - Outgoing: 2.
- Minimum Communications Range:
  - 900 m.
- All Communications Busses shall be Opto-Isolated to Provide Protection from High-Voltage Spikes;

Operating Environmental Conditions:
- Temperature Range: 0°C – 55°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

Indication:
- LEDs:
  - 3-LED Module Status Display;
  - 4-LED Status Display per Hub Output.

Mounting Options:
- Wall Mounting.

Enclosure:
- Colour: RAL9003, white;
- Each Output shall be labelled for Easy Identification;
- All Terminals shall be Removable for Ease of Wiring.

Features:
- On-Board Buttons to Manually Activate or Deactivate Each Hub Output;
- In-Field Firmware Upgrade via:
  - IDS-Bus.
- Divides the Bus into Four Completely Isolated Outputs:
  - One Input Port;
  - 2 Completely Isolated Output Ports.
- If One Output Fails, the Others will Continue to Function Independently.
- Mean Time Between Failures (MTBF): 50,000 Hours.
5.3.2.4 4-PROGRAMMABLE OUTPUT EXPANSION MODULE

The 4-Programmable Output Expansion Module shall be used to expand the number of hard wired outputs available on the Intruder Detection System and shall connect via the IDS-Bus.

The 4-Programmable Output Expansion Module shall comply with the following:

(l) Supply Characteristics:
- Bus Powered from the Control Panel:
  - Nominal Voltage: 12 VDC;
  - Voltage Range: 9 VDC – 16 VDC.
- Maximum Consumption:
  - Standby – 10 mA;
  - Alarm – 150 mA.
- The DC Input shall be Fused.

(m) Communication:
- Protocol (IDS_Bus):
  - RS-485.
- Number of Ports:
  - Incoming: 1;
- Minimum Communications Range:
  - 900 m.
- All Communications Busses shall be Opto-Isolated to Provide Protection from High-Voltage Spikes;

(n) Operating Environmental Conditions:
- Temperature Range: 0°C – 55°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(o) Indication:
- 3-LED Module Status Display:
  - PC;
  - Panel
  - RX/TX Status.
- 4-LED Output Status Display.

(p) Inputs & Outputs:
- Outputs:
  - 4 x Programmable Outputs;

(q) Mounting Options and Terminals:
- Wall Mounting;

(r) Removable Terminals for Fast, Secure, Orderly and Economic Installations;

(s) Enclosure:
- Colour: RAL9003, white;

(t) Certifications:
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
• Low Voltage Directive:
  ▪ EN 60950-1:2006/A12:2011;
  ▪ EN 45011 System 5:
  ▪ EN 50131-1:2006+A1;

(u) Features:
  • Connects Directly to the IDS-Bus;
  • In-Field Firmware Upgradeable via IDS-Bus;
  • Each Output shall be Labelled for Easy Identification;
  • It shall be Possible to Deactivate the 2-Way Wireless I/O after an Event or Timer;
  • Pulse Programmable Outputs for Fire Alarms.

(v) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.3 KEYPADS
5.3.3.1 LCD TOUCH SCREEN KEYPAD

The LCD Touch Screen Keypad shall be an interface to the Intruder Detection System and shall be capable of displaying all statuses from the system.

The keypad shall comply with the following specifications:

(a) Supply Characteristics:
  • Bus Powered from the Control Panel:
  • Nominal Voltage: 12 VDC;
  • Voltage Range: 9 VDC – 16 VDC.
  • Maximum Consumption:
    ▪ Standby – 50 mA;
    ▪ Alarm – 200 mA.
  • The DC Input shall be Fused.

(b) Communication:
  • Protocol (IDS_Bus):
    ▪ RS-485.
  • Number of Ports:
    ▪ Incoming: 1;
  • All Communications Busses shall be Opto-Isolated to Provide Protection from High-Voltage Spikes;

(c) Operating Environmental Conditions:
  • Temperature Range: 0°C – 55°C;
  • Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
  • Minimum IP Rating: IP55.

(d) Indication:
  • LED Status Display:
    ▪ Power;

(e) Mounting Options:
  • Wall Mounting.

(f) Enclosure Colour:
  • RAL 9011, black;
  • RAL 9003, white;
  • More Colours should be available on request of the Client.
(g) Display:
- Minimum Colour Depth: 16 bit;
- Minimum Size: 5”;
- Minimum Resolution: 480 x 270 pixels.

(h) Mean Time Between Failures (MTBF): 50,000 Hours.

The Touch Screen shall have all features and information on the entire Intruder Detection System available. From which alarm was triggered in which room, to the real time status of every area and zone in the installation, to any possible activity in the system.

5.3.4 DIRECT CONNECT INTERFACES FOR THE CONTROL PANEL

5.3.4.1 USB CONNECTOR

The USB Connector shall enable direct communication between the Intruder Detection System Control Panel and a PC.

The **USB Connector shall comply with the following specifications**:

(a) Supply Characteristics:
- Bus Powered from the Control Panel:
- Nominal Voltage: 5 VDC;
- Maximum Consumption:
  - Standby – 10 mA;
  - Operation – 60 mA.

(b) Communication:
- Protocol:
  - RS-232 on a DB-9 Connector;
  - USB.
- Number of Ports:
  - Incoming: 1;
  - Outgoing: 1.
- Minimum Communications Range:
  - 60 m.
- Minimum Available Communications Speeds:
  - 57.6k baud;
  - 38.4k baud;
  - 9.6k baud.

(c) Operating Environmental Conditions:
- Temperature Range: 0°C – 55°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
- Minimum IP Rating: IP54.

(d) Indication:
- 3 x LEDs:
  - PC;
  - Panel
  - RX/TX Status.
5.3.4.2 USB MEMORY KEY

The USB Memory Key shall enable direct Download or Upload of System Programming from the Software to the Intruder Detection System Control Panel without the need for a PC or any other Peripheral Device.

**The USB Connector shall comply with the following specifications:**

(a) Supply Characteristics :
   - Bus Powered from the Control Panel :
     - Nominal Voltage : 5 VDC;

(b) Communication :
   - Protocol :
     - USB,
   - Number of Ports : 1;

(c) Operating Environmental Conditions :
   - Temperature Range : 0°C – 55°C;
   - Relative Humidity : 5% – 90% Non-condensing Relative Humidity;
   - Minimum IP Rating : IP54.

(d) Indication :
   - 1 x LEDs :
     - Activity.

(e) Features :
   - Enables direct Control Panel Programming Upload or Download;
   - Lock Switch to Prevent Accidental Loss of Data.

(f) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.4.3 INTERNET MODULE

The Internet Module shall enable direct communication between the Intruder Detection System Control Panel and a PC.

**The Internet Module shall comply with the following specifications:**

(a) Supply Characteristics :
   - Bus Powered from the Control Panel :
     - Nominal Voltage : 12 VDC;
     - Maximum Consumption :
       - Standby – 10 mA;
       - Operation – 100 mA.

(b) Communication :
• Protocol:
  ▪ SSL;
  ▪ HTTPS.
• Number of Ports:
  ▪ Incoming: 1;
  ▪ Outgoing: 1.
• Minimum Communications Range:
  ▪ 90 m.
• Minimum Available Communications Speeds:
  ▪ 57.6k baud;
  ▪ 38.4k baud;
  ▪ 9.6k baud.
(c) Operating Environmental Conditions:
• Temperature Range: 0°C – 55°C;
• Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
• Minimum IP Rating: IP54.
(d) Inputs & Outputs:
• Two Programmable I/Os on Board Controlled via the Web Interface, Triggering an Email.
(e) Indication:
• 3 x LEDs:
  ▪ PC;
  ▪ Panel
  ▪ RX/TX Status.
(f) Enclosure:
• Colour: RAL9003, white;
(g) Each Output shall be Labelled for Easy Identification.
(h) Features:
• Enables Control Panel to Communicate and be Controlled with an Internet Connected Device;
• Receive Notification of System Alarms via Email;
• Arm/Disarm Individual Partitions via Web Browser;
• View Live Status of All Zones and Partitions via Web Browser;
• Connect on a Dynamic IP Address;
• Very Low Bandwidth Consumption.
(i) Mean Time Between Failures (MTBF): 50,000 Hours.

5.3.4.4 INTEGRATION MODULE

The Integration Module shall enable direct communication between the Intruder Detection System Control Panel and a Third Party Peripheral System.
The Integration Module shall comply with the following specifications:

(a) Supply Characteristics:
   - Bus Powered from the Control Panel:
   - Nominal Voltage: 5 VDC;
   - Maximum Consumption:
     - Standby – 10 mA;
     - Operation – 60 mA.

(b) Communication:
   - Protocol: USB:
     - ASCII;
     - C-BUS.
   - Number of Ports:
     - Incoming: 1;
     - Outgoing: 2.
   - Minimum Communications Range:
     - 10 m.

(c) Operating Environmental Conditions:
   - Temperature Range: 0°C – 55°C;
   - Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
   - Minimum IP Rating: IP54.

(d) Inputs & Outputs:
   - Two Programmable I/Os on Board Controlled via the Web Interface, Triggering an Email;
   - 16 Virtual Inputs to Trigger an Action in the Control Panel based on an Event Received from the Peripheral System using ASCII or C-BUS Protocol;
   - 30 Virtual Programmable I/O to Trigger an Action in the Peripheral System using ASCII or CBUS Protocol Based on an Event Received from the Control Panel

(e) Indication:
   - 3 x LEDs:
     - PC;
     - Panel
     - RX/TX Status.

(f) Certifications:
   - EMC Directive:
     - EN 61000-6-3:2007/A1:2011;
     - EN 50130-4:2011;
   - Low Voltage Directive:
     - EN 60950-1:2006/A12:2011;

(g) Enclosure:
   - Colour: RAL9003, white;

(h) Each Output shall be Labelled for Easy Identification.

(i) Features:
   - Enables Control Panel to Communicate and be Controlled with an Internet Connected Device;
   - Receive Notification of System Alarms via Email;
   - Arm/Disarm Individual Partitions via Web Browser;
   - View Live Status of All Zones and Partitions via Web Browser;
   - Connect on a Dynamic IP Address;
   - Very Low Bandwidth Consumption;
   - In-Field Firmware Upgradeable via USB;
   - 2048 Event Buffer;
   - Parallel and Serial Port for Printer Connections;
   - Provides an Interface between a Control Panel and a Third Party Peripheral System;
   - Automatically/Manually Print Reports of zones/systems Event via Printer and/or PC;
   - Assign to One or More Partitions.
5.3.5 CONNECTED DEVICES
5.3.5.1 DETECTORS
5.3.5.1.1 TYPE 1: WIRELESS PIR MOTION DETECTOR

The Motion Detector shall Detect All Intrusion and Transmit the Alarm to the Intruder Detection System Control Panel via Wireless Communication.

The Motion Detector shall comply with the following specifications:

(a) Supply Characteristics:
- Battery Powered:
- Minimum Battery Lifetime:
  - 3 Years.

(b) Communication:
- Protocol:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.
- Minimum Wireless Range:
  - 70 m in a Typical Residential Environment.

(c) Detection:
- Detection Channels:
  - 1 x Dual PIR.
- Detection Range and Viewing Angle:
  - 11 m x 11 m and Up To 15 m for Center Beams;
  - 88.5° Viewing Angle.
- Pet Immunity: Shall be Immune to Animals Weighing up to: 18 kg.

(d) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(e) Indication:
- 1 x LEDs:
  - Detection.

(f) Certifications:
- Security Grade:
  - EN 50131 – Grade 3;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
EN 45011 System 5 :
EN50131-1:2006+A1;
EN50131-3:2009;

(g) Features :

• Pet Immunity shall be Active for False Alarm Rejection in the Short and Medium Detection Ranges;
• Digital Detection Technology shall Deliver Improved Detection and False Alarm Rejection;
• High-Speed, Advanced Algorithm Digital Signal Processing to reduce False Alarms;
• Real Time Movement Analysis shall immediately Reject Non-Movement and reduce False Alarms;
• Digital EMI / RFI Interference Rejection for reduced False Alarms;
• Signal Energy Processing shall Measure the Energy from Each Detected Signal and Add these until a Minimum Required Level is Reached for Alarm;
• Automatic Temperature Compensation shall Automatically Adjust the Motion Detector’s Sensitivity According to the Difference between the Room Temperature and Body Temperature to reduce False Alarms;
• Dual Edge Processing shall Look at the Energy in Entry and Exit Signals and only Alarm once the required Energy Threshold is achieved to reduce False Alarms;
• Dual Opposed Detection shall compare the Entry and Exit Signals’ Polarity to that of a Movement Signal and thus reduce False Alarms.

(h) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.1.2 TYPE 2 : WIRELESS OUTDOOR DUAL PIR SIDE-VIEW DETECTOR

The Motion Detector shall Detect All Intrusion and Transmit the Alarm to the Intruder Detection System Control Panel via Wireless Communication.

The Motion Detector shall comply with the following specifications :

(a) Supply Characteristics :

• Battery Powered :
  ▪ 3 X Standard Alkaline Batteries – AA, 1.5 V (ANSI: 15A, IEC: LR6);
  ▪ Minimum Battery Lifetime :
    ▪ 3 Years.

(b) Communication :

• Protocol :
  ▪ Wireless-Bus.
• Available Frequencies :
  ▪ 433 MHz;
  ▪ 868 MHz.
• Minimum Wireless Range :
  ▪ 70 m in a Typical Residential Environment.

(c) Detection :

• Detection Channels :
  ▪ 2 x Dual PIR;
  ▪ with Eight Narrow Detection Beams.
- Detection Range and Viewing Angle:
  - 11 m x 11 m and Up To 15 m for Center Beams;
  - 88.5° Viewing Angle.
- Pet Immunity: Shall be Immune to Animals Weighing up to: 40 kg;
- Single or Dual Zone Operation Modes: Two Sides shall be capable of Reporting to a Single Zone or to Two Separate Zones.

(d) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(e) Indication:
- 1 x LEDs:
  - Detection.
- Buzzer for Audible Feedback.

(f) Certifications:
- Security Grade:
  - EN 50131 – Grade 3;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
  - EN 45011 System 5:
  - EN50131-1:2006+A1;
  - EN50131-3:2009;

(g) Tamper Detection – Dual:
- Removal of Cover;
- Removal of Unit.

(h) Features:
- Pet Immunity shall be Active for False Alarm Rejection in the Short and Medium Detection Ranges;
- Digital Detection Technology shall Deliver Improved Detection and False Alarm Rejection;
- High-Speed, Advanced Algorithm Digital Signal Processing to reduce False Alarms;
- Real Time Movement Analysis shall immediately Reject Non-Movement and reduce False Alarms;
- Digital EMI / RFI Interference Rejection for reduced False Alarms;
- Signal Energy Processing shall Measure the Energy from Each Detected Signal and Add these until a Minimum Required Level is Reached for Alarm;
- Automatic Temperature Compensation shall Automatically Adjust the Motion Detector’s Sensitivity According to the Difference between the Room Temperature and Body Temperature to reduce False Alarms;
- Dual Edge Processing shall Look at the Energy in Entry and Exit Signals and only Alarm once the required Energy Threshold is achieved to reduce False Alarms;
- Dual Opposed Detection shall compare the Entry and Exit Signals’ Polarity to that of a Movement Signal and thus reduce False Alarms;
- Shall have a Very High White Light Rejection;
- In-Field Firmware Upgradable via Serial Port;
- 3-Minute Energy Saving Mode after Two Detections within a Five-Minute Period;
• Lenses shall be UV Protected for Outdoor use;
• The Casing shall be Impact and Temperature Resistant.

(i) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.1.3 TYPE 3 : WIRELESS INDOOR / OUTDOOR WINDOW AND SLIDING DOOR PIR DETECTOR

The Motion Detector shall Detect All Intrusion and Transmit the Alarm to the Intruder Detection System Control Panel via Wireless Communication.

The Motion Detector shall comply with the following specifications :

(a) Supply Characteristics :
• Battery Powered :
  ▪ 3 X Standard Alkaline Batteries – AA, 1.5 V (ANSI: 15A, IEC: LR6);
• Minimum Battery Lifetime :
  ▪ 3 Years.

(b) Communication :
• Protocol :
  ▪ Wireless-Bus.
• Available Frequencies :
  ▪ 433 MHz;
  ▪ 868 MHz.
• Minimum Wireless Range :
  ▪ 70 m in a Typical Residential Environment.

(c) Detection :
• Detection Channels :
  ▪ 1 x Dual PIR;
• Detection Range and Viewing Angle :
  ▪ Pet Immunity Mode : 7.5 m x 2 m;
  ▪ Indoor Mode : 10 m x 2 m;
  ▪ Narrow Beam : 0.5 m Wide at 5 m.
• Pet Immunity : Shall be Immune to Animals Weighing up to : 40 kg;
• Integrated Creep Zone Detection.

(d) Operating Environmental Conditions :
• Temperature Range : -20°C – 50°C;
• Relative Humidity : 5% – 90% Non-condensing Relative Humidity;
• Minimum IP Rating : IP55.

(e) Indication :
• 1 x LEDs :
  ▪ Detection.
• Buzzer for Audible Feedback.

(f) Certifications :
• Security Grade:
  ▪ EN 50131-2-2 – Grade 2;
• Environmental Grade:
  ▪ EN 50130-5 – Class II;
• EMC Directive :
  ▪ EN 61000-6-3:2007/A1:2011;
- EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
  - EN 45011 System 5:
    - EN50131-1:2006+A1;
    - EN50131-3:2009;

(g) Tamper Detection – Dual:
- Removal of Cover;
- Removal of Unit.

(h) Features:
- Pet Immunity shall be Active for False Alarm Rejection in the Short and Medium Detection Ranges;
- Digital Detection Technology shall Deliver Improved Detection and False Alarm Rejection;
- High-Speed, Advanced Algorithm Digital Signal Processing to reduce False Alarms;
- Real Time Movement Analysis shall immediately Reject Non-Movement and reduce False Alarms;
- Digital EMI / RFI Interference Rejection for reduced False Alarms;
- Signal Energy Processing shall Measure the Energy from Each Detected Signal and Add these until a Minimum Required Level is Reached for Alarm;
- Automatic Temperature Compensation shall Automatically Adjust the Motion Detector’s Sensitivity According to the Difference between the Room Temperature and Body Temperature to reduce False Alarms;
- Dual Edge Processing shall Look at the Energy in Entry and Exit Signals and only Alarm once the required Energy Threshold is achieved to reduce False Alarms;
- Dual Opposed Detection shall compare the Entry and Exit Signals’ Polarity to that of a Movement Signal and thus reduce False Alarms;
- Shall have a Very High White Light Rejection;
- In-Field Firmware Upgradable via Serial Port;
- 3-Minute Energy Saving Mode after Two Detections within a Five-Minute Period;
- Lens shall be UV Protected for Outdoor use;
- The Casing shall be Impact and Temperature Resistant.

(i) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.1.4 TYPE 4 : WIRELESS INDOOR DUAL PIR DETECTOR

The Motion Detector shall Detect All Intrusion and Transmit the Alarm to the Intruder Detection System Control Panel via Wireless Communication.

**The Motion Detector shall comply with the following specifications:**

(a) Supply Characteristics:
- Battery Powered:
  - 3 X Standard Alkaline Batteries – AA, 1.5 V (ANSI: 15A, IEC: LR6);
- Minimum Battery Lifetime:
  - 3 Years.
(b) Communication:
- Protocol:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.
- Minimum Wireless Range:
  - 70 m in a Typical Residential Environment.

(c) Detection:
- Detection Channels:
  - 1 x Dual PIR;
- Detection Range and Viewing Angle:
  - 11 m x 11 m;
  - 90° Viewing Angle.
- Pet Immunity: Shall be Immune to Animals Weighing up to: 40 kg.

(d) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(e) Indication:
- 1 x LEDs:
  - Detection.
- Buzzer for Audible Feedback.

(f) Certifications:
- Security Grade:
  - EN 50131 – Grade 2;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
- EN 45011 System 5:
  - EN50131-1:2006+A1;
  - EN50131-3:2009;

(g) Tamper Detection – Dual:
- Removal of Cover;
- Removal of Unit.

(h) Features:
- Pet Immunity shall be Active for False Alarm Rejection in the Short and Medium Detection Ranges;
- Digital Detection Technology shall Deliver Improved Detection and False Alarm Rejection;
- High-Speed, Advanced Algorithm Digital Signal Processing to reduce False Alarms;
- Real Time Movement Analysis shall immediately Reject Non-Movement and reduce False Alarms;
- Digital EMI / RFI Interference Rejection for reduced False Alarms;
- Signal Energy Processing shall Measure the Energy from Each Detected Signal and Add these until a Minimum Required Level is Reached for Alarm;
• Automatic Temperature Compensation shall Automatically Adjust the Motion Detector’s Sensitivity According to the Difference between the Room Temperature and Body Temperature to reduce False Alarms;
• Dual Edge Processing shall Look at the Energy in Entry and Exit Signals and only Alarm once the required Energy Threshold is achieved to reduce False Alarms;
• Dual Opposed Detection shall compare the Entry and Exit Signals’ Polarity to that of a Movement Signal and thus reduce False Alarms;
• Shall have a Very High White Light Rejection;
• In-Field Firmware Upgradable via Serial Port;
• 3-Minute Energy Saving Mode after Two Detections within a Five-Minute Period.

(i) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.1.5 TYPE 5 : WIRELESS OUTDOOR DUAL PIR DETECTOR

The Motion Detector shall Detect All Intrusion and Transmit the Alarm to the Intruder Detection System Control Panel via Wireless Communication.

The Motion Detector shall comply with the following specifications :

(a) Supply Characteristics :
• Battery Powered :
  ▪ 3 X Standard Alkaline Batteries – AA, 1.5 V (ANSI: 15A, IEC: LR6);
• Minimum Battery Lifetime :
  ▪ 3 Years.
(b) Communication :
• Protocol :
  ▪ Wireless-Bus.
• Available Frequencies :
  ▪ 433 MHz;
  ▪ 868 MHz.
• Minimum Wireless Range :
  ▪ 70 m in a Typical Residential Environment.
(c) Detection :
• Detection Channels :
  ▪ 2 x Dual PIR;
• Detection Range and Viewing Angle :
  ▪ Pet Immunity Mode : 11 m x 11 m with an 85° Viewing Angle;
  ▪ Corridor Mode : 13 m x 2 beams with a 5.64° viewing angle.
• Pet Immunity : Shall be Immune to Animals Weighing up to : 40 kg.
(d) Operating Environmental Conditions :
• Temperature Range : -20°C – 50°C;
• Relative Humidity : 5% – 90% Non-condensing Relative Humidity;
• Minimum IP Rating : IP55.
(e) Indication :
• 1 x LEDs :
  ▪ Detection.
• Buzzer for Audible Feedback.
(f) Certifications :
• Security Grade:
  ▪ EN 50131 – Grade 2;
• Environmental Grade:
  ▪ EN 50130-5 – Class II;
• EMC Directive :
  ▪ EN 61000-6-3:2007/A1:2011;
  ▪ EN 50130-4:2011;
• Low Voltage Directive :
  ▪ EN 60950-1:2006/A12:2011;
• RTTE Directive :
  ▪ EN 300 220-2 V2.4.1 – 3(2);
  ▪ EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
  ▪ EN 45011 System 5 :
    ▪ EN50131-1:2006+A1;
    ▪ EN50131-3:2009;

(g) Tamper Detection – Dual :
• Removal of Cover;
• Removal of Unit.

(h) Features :
• Pet Immunity shall be Active for False Alarm Rejection in the Short and Medium Detection Ranges;
• Digital Detection Technology shall Deliver Improved Detection and False Alarm Rejection;
• High-Speed, Advanced Algorithm Digital Signal Processing to reduce False Alarms;
• Real Time Movement Analysis shall immediately Reject Non-Movement and reduce False Alarms;
• Digital EMI / RFI Interference Rejection for reduced False Alarms;
• Signal Energy Processing shall Measure the Energy from Each Detected Signal and Add these until a Minimum Required Level is Reached for Alarm;
• Automatic Temperature Compensation shall Automatically Adjust the Motion Detector’s Sensitivity According to the Difference between the Room Temperature and Body Temperature to reduce False Alarms;
• Dual Edge Processing shall Look at the Energy in Entry and Exit Signals and only Alarm once the required Energy Threshold is achieved to reduce False Alarms;
• Dual Opposed Detection shall compare the Entry and Exit Signals’ Polarity to that of a Movement Signal and thus reduce False Alarms;
• Shall have a Very High White Light Rejection;
• In-Field Firmware Upgradable via Serial Port;
• 3-Minute Energy Saving Mode after Two Detections within a Five-Minute Period;
• Lens shall be UV Protected for Outdoor use;
• The Casing shall be Impact and Temperature Resistant.

(i) Mean Time Between Failures (MTBF) : 50,000 Hours.
5.3.5.1.6 TYPE 6 : WIRELESS MULTI-AXIS MOTION DETECTOR

The Motion Detector shall Detect All Movement on Tagged Items and Transmit the Alarm to the Intruder Detection System Control Panel via Wireless Communication.

The Motion Detector shall comply with the following specifications :

(a) Supply Characteristics :
   • Battery Powered :
     ▪ 1 X Standard Lithium Coin Battery – CR 2032, 3.0 V (ANSI: 5004LC);
     ▪ Minimum Battery Lifetime :
       ▪ 2 Years with two Detections per Week.

(b) Communication :
   • Protocol :
     ▪ Wireless-Bus.
   • Available Frequencies :
     ▪ 433 MHz;
     ▪ 868 MHz.
   • Minimum Wireless Range :
     ▪ 70 m in a Typical Residential Environment.

(c) Detection :
   • Detection Channels :
     ▪ Three-Axis (X, Y, and Z Axis) Accelerometer Detection;
   • Sensitivity : Shall be Fully Adjustable :
     ▪ Short Movement (High Security) = 1 – 3 seconds;
     ▪ Long Movement (Standard Security) = 3 – 5 seconds;
     ▪ An Additional Grace Period shall be possible.

(d) Operating Environmental Conditions :
   • Temperature Range : -20°C – 50°C;
   • Relative Humidity : 5% – 90% Non-condensing Relative Humidity;
   • Minimum IP Rating : IP55.

(e) Indication :
   • 1 x LEDs :
     ▪ Detection.
     ▪ Buzzer for Audible Feedback.

(f) Typical Dimensions: 12.5cm x 4.6cm x 2.5cm

(g) Certifications :
   • Security Grade:
     ▪ EN 50131 – Grade 2;
   • Environmental Grade:
     ▪ EN 50130-5 – Class II;
   • EMC Directive :
     ▪ EN 61000-6-3:2007/A1:2011;
     ▪ EN 50130-4:2011;
   • Low Voltage Directive :
     ▪ EN 60950-1-2006/A12:2011;
   • RTTE Directive :
     ▪ EN 300 220-2 V2.4.1 – 3(2);
     ▪ EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
     ▪ EN 45011 System 5 :
       ▪ EN50131-1:2006+A1;
       ▪ EN50131-3:2009;

(h) Tamper Detection – Dual:
- Removal of Cover;
- Removal of Unit.

(i) Features:
- Real Time Movement Analysis shall immediately Reject Non-Movement and reduce False Alarms;
- Digital EMI / RFI Interference Rejection for reduced False Alarms;
- Signal Energy Processing shall Measure the Energy from Each Detected Signal and Add these until a Minimum Required Level is Reached for Alarm;
- Dual Edge Processing shall Look at the Energy in Entry and Exit Signals and only Alarm once the required Energy Threshold is achieved to reduce False Alarms;
- In-Field Firmware Upgradable via Serial Port;
- 3-Minute Energy Saving Mode after Two Detections within a Five-Minute Period;
- Low Battery and RF Supervision;
- Power Saving Mode shall be available to Conserves Battery Life.

(j) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.2 WIRELESS I/O
5.3.5.2.1 2-WAY WIRELESS I/O


The 2-Way Wireless I/O shall comply with the following specifications:

(a) Supply Characteristics:
- DC Voltage Range : 5 VDC – 30 VDC;
- AC Voltage Range : 6 VAC – 16.5 VAC;
- The AC/DC Input shall be Fused.
- Battery Powered:
  - 2 X Standard Alkaline Batteries – AAA, 1.5 V (ANSI: 24A, IEC: LR03);
- Minimum Battery Lifetime:
  - 3 Years.

(b) Communication:
- Protocol:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.
- Minimum Wireless Range:
  - 70 m in a Typical Residential Environment.

(c) Operating Environmental Conditions:
- Temperature Range : -20°C – 50°C;
- Relative Humidity : 5% – 90% Non-condensing Relative Humidity;

(d) Inputs & Outputs:
- Inputs:
  - Universal Transmitter Input (N.O. or N.C.).
- Outputs:
1 x Fully Programmable 5A Relay Output.

(e) Indication :
- 1 x LEDs :
  - Detection.
- Buzzer for Audible Feedback.

(f) Typical Dimensions:
- 125 mm x 45 mm x 25 mm.

(g) Certifications :
- Security Grade:
  - EN 50131 – Grade 2;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive :
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive :
  - EN 60950-1:2006/A12:2011;
- RTTE Directive :
  - EN 300 220 – V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);

(h) Tamper Detection :
- Removal of Cover.

(i) Features :
- The 2-Way Communication shall Allow the 2-Way Wireless I/O To Receive Commands from Control Panel and then Confirm the Command;
- Optional Activation of the 2-Way Wireless I/O Output if All Communication Between the Control Panel and the 2-Way Wireless I/O is lost;
- It shall be possible to Deactivate the 2-Way Wireless I/O after an Event or Timer.

(j) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.3 WIRELESS DOOR CONTACTS (DPS)
5.3.5.3.1 2-ZONE LONG-RANGE WIRELESS DOOR CONTACT

The Wireless Door Contact shall remotely Transmit DPS and Other Alarms to the Intruder Detection System Control Panel via Wireless Communication.

The Wireless Door Contact shall comply with the following specifications :

(a) Supply Characteristics :
- Battery Powered :
  - 2 X Standard Alkaline Batteries – AAA, 1.5 V (ANSI: 24A, IEC: LR03);
- Minimum Battery Lifetime :
  - 3 Years.
(b) Communication :
- Protocol :
  - Wireless-Bus.
- Available Frequencies :
- 433 MHz;
- 868 MHz.
- Minimum Wireless Range:
  - 100 m in a Typical Residential Environment.
(c) Detection:
- Dual Reed Switches open when magnet is moved;
(d) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;
(e) Inputs & Outputs:
- Inputs:
  - Zone 1: Reed Switches for DPS;
  - Zone 2: Universal Transmitter Input (N.O. or N.C.);
- Inputs shall be Independently Zoned.
(f) Indication:
- 1 x LEDs:
  - Low Battery;
  - Signal Transmission.
(g) Typical Dimensions:
- 125 mm x 45 mm x 35 mm.
(h) Certifications:
- Security Grade:
  - EN 50131 – Grade 2;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
(i) Tamper Detection:
- Removal of Cover.
(j) Mean Time Between Failures (MTBF): 50,000 Hours.

### 5.3.5.3.2 2-ZONE MEDIUM-RANGE WIRELESS DOOR CONTACT

The Wireless Door Contact shall remotely Transmit DPS and Other Alarms to the Intruder Detection System Control Panel via Wireless Communication.
The Wireless Door Contact shall comply with the following specifications:

(a) Supply Characteristics:
- Battery Powered:
  - 2 X Standard Alkaline Batteries – AAA, 1.5 V (ANSI: 24A, IEC: LR03);
- Minimum Battery Lifetime:
  - 3 Years.

(b) Communication:
- Protocol:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.
- Minimum Wireless Range:
  - 70 m in a Typical Residential Environment.

(c) Detection:
- Dual Reed Switches open when magnet is moved;

(d) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(e) Inputs & Outputs:
- Inputs:
  - Zone 1: Reed Switches for DPS;
  - Zone 2: Universal Transmitter Input (N.O. or N.C.);
- Inputs shall be Independently Zoned.

(f) Indication:
- 1 x LEDs:
  - Low Battery;
  - Signal Transmission.

(g) Typical Dimensions:
- 110 mm x 35 mm x 25 mm.

(h) Certifications:
- Security Grade:
  - EN 50131 – Grade 2;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);

(i) Tamper Detection:
- Removal of Cover.

(j) Mean Time Between Failures (MTBF): 50,000 Hours.
5.3.5.3.3 2-ZONE SHORT-RANGE WIRELESS DOOR CONTACT

The Wireless Door Contact shall remotely Transmit DPS and Other Alarms to the Intruder Detection System Control Panel via Wireless Communication.

The Wireless Door Contact shall comply with the following specifications:

(a) Supply Characteristics:
- Battery Powered:
  - 2 X Standard Alkaline Batteries – AAA, 1.5 V (ANSI: 24A, IEC: LR03);
  - Minimum Battery Lifetime:
    - 3 Years.

(b) Communication:
- Protocol:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.
- Minimum Wireless Range:
  - 40 m in a Typical Residential Environment.

(c) Detection:
- Single Reed Switch opens when magnet is moved;

(d) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(e) Typical Dimensions:
- 45 mm x 35 mm x 20 mm.

(f) Certifications:
- Security Grade:
  - EN 50131 – Grade 2;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);

(g) Tamper Detection:
- Removal of Cover.

(h) Mean Time Between Failures (MTBF): 50,000 Hours.
5.3.5.4 REMOTE CONTROLS
5.3.5.4.1 ERGONOMIC REMOTE CONTROL

The Remote Control shall remotely Transmit Commands to the Intruder Detection System Control Panel via Wireless Communication.

The Wireless Door Contact shall comply with the following specifications:

(a) Supply Characteristics:
   - Battery Powered:
     - 1 X Standard Lithium Coin Battery – CR 2032, 3.0 V (ANSI: 5004LC);
     - Minimum Battery Lifetime:
       - 3 Years.

(b) Communication:
   - Protocol:
     - Wireless-Bus.
   - Available Frequencies:
     - 433 MHz;
     - 868 MHz.
   - Minimum Wireless Range:
     - 60 m in a Typical Residential Environment.

(c) Operating Environmental Conditions:
   - Temperature Range: -20°C – 50°C;
   - Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(d) Typical Dimensions:
   - 60 mm x 35 mm x 15 mm.

(e) Certifications:
   - Security Grade:
     - EN 50131 – Grade 2;
   - Environmental Grade:
     - EN 50130-5 – Class II;
   - EMC Directive:
     - EN 61000-6-3:2007/A1:2011;
     - EN 50130-4:2011;
   - Low Voltage Directive:
     - EN 60950-1:2006/A12:2011;
   - RTTE Directive:
     - EN 300 220-2 V2.4.1 – 3(2);
     - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
   - Use of Certain Hazardous Substances in Electrical and Electronic Equipment:

(f) Features:
   - The Remote shall have a Slim, Ergonomic Design;
   - The Remote shall be Water Resistant;
   - The Remote shall be Capable of Performing up to 5 Different Actions.

(g) Mean Time Between Failures (MTBF): 50,000 Hours.

5.3.5.4.2 TYPE 1 : MULTI-BUTTON 2-WAY REMOTE CONTROL

The Wireless Door Contact shall comply with the following specifications:

(a) Supply Characteristics:
- Battery Powered:
  - 1 X Standard Lithium Coin Battery – CR 2032, 3.0 V (ANSI: 5004LC);
- Minimum Battery Lifetime:
  - 3 Years.

(b) Communication:
- Protocol:
  - Wireless-Bus.
- Available Frequencies:
  - 433 MHz;
  - 868 MHz.
- Minimum Wireless Range:
  - 45 m in a Typical Residential Environment.

(c) Operating Environmental Conditions:
- Temperature Range: -20°C – 50°C;
- Relative Humidity: 5% – 90% Non-condensing Relative Humidity;

(d) Indication:
- 1 x Multi Coloured LED:
  - Low Battery;
  - System Status.
- Buzzer:
  - System Status.

(e) Typical Dimensions:
- 60 mm x 35 mm x 15 mm.

(f) Certifications:
- Security Grade:
  - EN 50131 – Grade 2;
- Environmental Grade:
  - EN 50130-5 – Class II;
- EMC Directive:
  - EN 61000-6-3:2007/A1:2011;
  - EN 50130-4:2011;
- Low Voltage Directive:
  - EN 60950-1:2006/A12:2011;
- RTTE Directive:
  - EN 300 220-2 V2.4.1 – 3(2);
  - EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
- Use of Certain Hazardous Substances in Electrical and Electronic Equipment:

(g) Features:
- The Remote shall have a Slim, Ergonomic Design;
- The Remote shall be Water Resistant;
• The Remote shall have Back Lit Buttons;
• The Remote shall be Capable of Receiving and Displaying the System Status;
• The Remote shall have a Label to Identify the Remote Control Owner;
• The Remote shall Provide Visual and Auditory Feedback of System Status;
• The Remote shall be Capable of Performing up to 6 Different Actions.

(h) Mean Time Between Failures (MTBF) : 50,000 Hours.

5.3.5.4.3 TYPE 2 : MULTI-BUTTON 2-WAY REMOTE CONTROL


The Wireless Door Contact shall comply with the following specifications :

(i) Supply Characteristics :
• Battery Powered :
  ▪ 1 X Standard Lithium Coin Battery – CR 2032, 3.0 V (ANSI: 5004LC);
• Minimum Battery Lifetime :
  ▪ 3 Years.

(j) Communication :
• Protocol :
  ▪ Wireless-Bus.
• Available Frequencies :
  ▪ 433 MHz;
  ▪ 868 MHz.
• Minimum Wireless Range :
  ▪ 45 m in a Typical Residential Environment.

(k) Operating Environmental Conditions :
• Temperature Range : -20°C – 50°C;
• Relative Humidity : 5% – 90% Non-condensing Relative Humidity;
• Minimum IP Rating : IP55.

(l) Indication :
• 1 x Multi Coloured LED :
  ▪ Low Battery;
  ▪ System Status.
• Buzzer :
• System Status.
  ▪ Partition LEDs :
• Partition 1 LEDs = Signal Strength Display;
• Partition 2 LEDs = RF Interference Display.

(m) Typical Dimensions:
• 80 mm x 35 mm x 15 mm.

(n) Certifications :
• Security Grade:
  ▪ EN 50131 – Grade 2;
• Environmental Grade:
  ▪ EN 50130-5 – Class II;
• EMC Directive :
▪ EN 61000-6-3:2007/A1:2011;
▪ EN 50130-4:2011;
• Low Voltage Directive :
  ▪ EN 60950-1:2006/A12:2011;
• RTTE Directive :
  ▪ EN 300 220-2 V2.4.1 – 3(2);
  ▪ EN 301 489-1 V1.9.2; EN 301 489-3 V1.4.1 – 3(1)(b);
• Use of Certain Hazardous Substances in Electrical and Electronic Equipment :
  ▪ EN 50581:2012.

(o) Features :
• The Remote shall have a Compact Design;
• The Remote shall be Water Resistant;
• The Remote shall have Back Lit Buttons;
• The Remote shall be Capable of Receiving and Displaying the System Status;
• The Remote shall have a Label to Identify the Remote Control Owner;
• The Remote shall Provide Visual and Auditory Feedback of System Status;
• The Remote shall have a System Status Memory. The Remote shall Save the Last System Status Received from the Control Panel in Memory. Momentarily Pressing the Info Button shall Display the Last System Status, Even when Out of Range. This Function shall be Used to Confirm the Last Action performed on the System While Away from the System.
• Modes :
  ▪ Keypad Mode : Requires Code Entry;
  ▪ Remote Mode : One-Touch Arming / Disarming.
• The Remote shall be Capable of Handling Multiple Partitions;
• The Remote shall be Capable of Performing up to 6 Different Actions.

(p) Mean Time Between Failures (MTBF) : 50,000 Hours.
7 IP INTERCOM SYSTEMS

7.1 GENERAL

The system shall consist of a full duplex intercommunication system to provide digital voice communication, voice recording and event logging facilities.

The Digital Intercom sub-system hardware shall be integrated with the PSIM via a High Level Interface (HLI).

The full functionality of the system shall be integrated with the PSIM to provide enhanced features including but not limited to:

(a) Station Call-In
(b) Station Fault Analysis
(c) Call In Divert
(d) Call Answer
(e) Call Cancel
(f) Call-In Queuing
(g) Tamper Alarm monitoring
(h) Threshold Monitoring (Disturbance detection)
(i) Individual Station Speaker and Microphone sensitivity adjustment
(j) Page All

The IP Intercom system shall enable the selection of any individual or group of intercom stations by any operator workstation within the campus.

The following functional features shall be provided by the proposed system:

(a) Noise Immunity:
   • The system shall provide clear undistorted speech and music transmission (Integrated noise cancelation).
   • The audio signal shall be digitally transmitted to each intercom station to provide immunity against electrical and earthing interference typically associated with analogue systems.

(b) Structured Cabling:
   • Standard 10/100/1000 based Ethernet backbone (IEEE 802.3af) with POE with independent CAT-6 cabling per station (provided by others).

(c) Multiple Audio Channels:
   • The system shall be capable of transmitting a minimum of three digitized audio channels simultaneously, which shall enable intercom stations to independently select either a music channel, an education channel or to call and communicate with the system operator. The channel selection and current operation of one station shall have no effect on the channel selection and operation of any other station.

(d) Interface to the Telephone Network:
   • The system shall have the capability of interfacing to the campus telephone system (IP PBX), which will enable existing telephones situated in offices to Page intercom stations.

(e) Tamper Detection:
   • Each intercom station shall provide tamper detection, which shall automatically notify the system operator of an intercom station, which has been opened or tampered with in any way.

(f) PC based Operator Consoles:
   • A dedicated PC based operator console shall be provided at each local control room and at the Central control station. It shall be possible for any operator console to call any intercom station within the entire campus based upon authorized user levels. In the...
case of failure of any operator console it shall be possible to route incoming calls from intercom stations to any other operator console in the campus.

(g) Event Recording and Reporting:
- The system shall be capable of recording and reporting the following events with an accompanying time and date stamp:
  - Intercom station call requests with station identification;
  - Operator response with operator/station identification and call duration.

(h) Voice Recording:
- 32 Channels simultaneous recording.
- Emergency calls shall be recorded onto a PC hard drive. System operators shall be able to replay the emergency call via a PC based control system, which shall indicate the associated intercom station and time and date of the call.

(i) Two Way Conversations:
- The system operators shall be provided with handsets, which shall enable bi-directional conversations with any selected intercom station by means of an integrated Push to Talk Function.

(j) Volume Level Adjustment:
- The system shall enable operators to independently set the speaker volume and microphone sensitivity levels for each intercom station in order to optimize the acoustic settings for each building or room via IP interface.

(k) VoIP Compatibility (Ethernet Telephones):
- The system shall be compatible with SIP protocol as a minimum and will enable standard Voice over IP telephone systems to be connected to the network, which will enable the expansion or replacement of equipment with products from a variety of competitors. The system shall be able to transmit multiple audio conversations between buildings via existing Ethernet networks.
- All substations will be SIP compatible VoIP stations.

7.2 SYSTEM DESCRIPTION

(a) The system shall be compatible with standard voice over IP products (IP Telephony), which employ such protocols as SIP, and be capable of communicating both data and audio signals over standard TCP/IP and UDP Protocols. Where possible the system should make use of existing Large Area Networks for the transmission of control and Audio data.

(b) The exchange Server shall include 2 Ethernet IP ports which support protocols IP v4-IP v6, TCP, UDP, Telnet, FTP, NTP, HTTP 1.1, Syslog, SNMP v2c, SIP, RTP, RTCP, VoIP.

(c) The overall design of the system software and cabling shall be such that as far as practical, failure of one part (building) of the system does not affect normal operation of any other part of the system. Thus any node in any position on the network that fails, will not disrupt the integrity of the network in any way.

(d) The system shall employ duplex digital audio technology and provide clear undistorted speech communications, free from background noise and/or external interference.

(e) The system shall be capable of transmitting at least 32 simultaneous full duplex conversations via the TCP/IP network.

(f) The intercom system shall be capable of being fully integrated with a PC based Graphical User Interface (GUI) via a bi-directional high level interface to allow remote monitoring of all intercom station calls by the GUI. All such interfacing of systems shall be configured such that if any one system fails to operate, the other systems shall continue to operate without any detrimental effect.

(g) A dedicated GUI for the control, monitoring and logging of events shall be provided for the intercom system, and shall be installed at each control centre.

(h) The system shall be able to incorporate a redundancy server, via IP, which will automatically take over the duties of the main server should it go faulty. Both the Main Server and the Redundancy Server must support wideband audio (7 kHz), built in firewall, integrated web & SIP server as well as low latency switching. Both servers shall allow for remote programming, logging, maintenance and statistical information via IP using the web browser.
(i) The system shall be able to communicate with any other intercom server or exchange by using transparent dialling between local and remote modules.
(j) All necessary data and audio routing between the server shall be via IP and only require the necessary VoIP software licences based on the system design. No additional hardware, PCB’s or proprietary black boxes shall be necessary to do the networking via IP between servers.

7.3 INTERCOM OPERATIONS

7.3.1 AUDIO CONTROL – INTERCOM ICON

The PSIM shall provide a control icon with visual status indication for each intercom station within the entire campus.

The icons shall be used to initiate or terminate an audio channel between the relevant control room operator’s audio console and the selected intercom station.

Each Intercom station icon shall provide interaction with the mouse by indicating status changes and alarms graphically when clicked.

The alarm detail displayed by the GUI shall include:

(k) Intercom station Tamper alarm
(l) Intercom station Threshold alarm
(m) Intercom station I/O alarm
(n) Intercom station Communications alarm
(o) Intercom busy
(p) Intercom waiting

All alarm conditions shall be presented to the operator within a fault queue as described in the PSIM specification.

A right mouse click over any icon shall provide the operator with an option to acknowledge an alarm condition, to inhibit an intercom station, or to view the engineering properties of the element provided the necessary user level is active. Inhibiting an intercom station shall change the icon colour to blue.

Intercom Station Call In:

(a) Activating a station icon shall open a talk path between the operator and the associated intercom station. The associated status icon shall illuminate yellow to indicate an active channel.
(b) Activating the staff station icon a second time shall close the talk path and the status icon shall extinguish.

Automatic Termination of an Audio Channel:

(a) Should multiple audio call in’s be received by the local operator, the operator shall only be required to select each audio icon once. The second icon selected shall initiate an audio channel to the appropriate intercom station and initiate an automatic de-select command to the previous channel.
Delayed Call-In:

(a) Upon activation of a station call-in button on an intercom station which falls under the control of a local control workstation, provided the particular operator is logged in, the call shall at first be routed to the local operator. If the local operator fails to respond to a call in within 60 seconds, the call is automatically routed to central control. This event is to be logged to the event recording system.

Audio Queue:

(b) An Audio Call-in queue facility shall be provided as an integrated function of the PSIM system. Refer to the PSIM specification

7.4 INTERCOM STATIONS

(a) The contractor shall supply, install and commission a networked passage door Intercom System to the locations nominated in the accompanying drawings. Monitoring locations shall be provided in each local control room, with the primary central monitoring location to be installed in the Central Control room.

(b) Calls originated from passage door intercom stations shall be routed to the respective local control room GUI Operator terminal and Intercom GUI.

(c) A Call diversion facility in the event of un-answered or unattended mode shall be provided, and shall be configured.

(d) All calls between Control Stations and Intercom Stations shall be able to be digitally recorded on the Intercom Digital Recording System.

(e) The Digital Recording System shall be expandable to cater for future system expansion.

7.5 SYSTEM OF OPERATION

7.5.1 GENERAL

Within each nominated building, (for this tender it will be the test lab) the contractor shall supply and install an integrated IP intercom system. The system shall be complete with IP Intercom Stations, PBX controllers to provide voice communications to the local control room and/or the Central Control Room.

The PBX used on the Campus is Microsoft Lync. Licenses will be procured through the Sol Plaatje University Microsoft Licensing Agreement.

The system shall provide the following minimum System Functions:

7.5.1.1 NORMAL CALLS

Calls initiated from Intercom stations to system operators or vice versa.

7.5.1.2 ALARM CALLS

Emergency calls initiated by security officers or automatically triggered by system events such as audio level alarms (Threshold monitoring).

7.5.1.3 TAMPER CALLS

Tamper calls initiated when an attempt is made to gain unauthorized access to intercom station electronics
7.5.1.4 SYSTEM ERROR MESSAGES AND EVENT LOGGING

System errors and disturbances shall be displayed on appropriately configured operator workstations according the type and location of the error or event. Disturbances such as raised voice levels shall automatically generate alarms, which shall be documented in a log file and on a printer. Log files shall be named and stored by date.

The current or historical log files shall be displayed on the screen or printed out on request. The system shall maintain log files for a minimum of six months. The system shall provide the operator with a warning prompt indicating the files should be backed up if required for a longer duration. System functionality shall not be influenced in the event of failure of any one part of the system or operator station. Each operator workstation shall be configured as an autonomous system. In the event of an operator system failure, the functionality of that station shall be transferred to another operator workstation on the system according to a pre-configured set of rules.

The current or historical log files shall be displayed on the screen or printed out on request. The system shall maintain log files for a minimum of six months. The system shall provide the operator with a warning prompt indicating the files should be backed up if required for a longer duration.

7.5.1.5 DATA INTEGRITY

In the event of power failure, the actual status information in the system at the time of the failure shall not be lost. When the power is reconnected, all status information at the time of the power failure shall be retrievable and will be displayed on the relevant screens.

7.5.1.6 LISTEN-IN

A “Listen-In” function shall be provided, and configured in accordance with the engineer’s specification, to provide either overt or covert operation or to be disabled altogether.

Call Monitor

A Call Monitor facility shall be provided, which shall provide the operator with station identification. The call monitor shall display the calls and events from individual intercom stations in a priority based text listing.

The Call Monitor function shall be capable of displaying the following information:

(f) Normal Calls;
(g) Tamper Calls;
(h) Alarm Calls;
(i) Guard Present;
(j) Intercom Station Error;
(k) Intercom Station Failure.

It shall be possible to configure the call or event priority on the operator GUI.

7.5.1.7 ESTABLISHING A CALL

At a minimum the system shall be capable of establishing calls in the following two ways:

...
7.5.1.7.1 RESPOND TO NORMAL CALLS

Call-ins shall be entered into Call-in queue on a first in – first out (FIFO) bases, and sorted by priority level. Priority levels shall be set for each intercom station on the system. On receiving a call-in the operator shall only need make a single keystroke to answer the highest priority call that has been in the queue for the longest period of time. It shall also be possible to select a specific call-in and initiate a call by making a single keystroke.

7.5.1.7.2 RESPONSE TO ALARM CALLS

The system shall be capable of automatically detecting raised audio levels at nominated intercom stations. It shall be possible to configure the system to automatically initiate calls to intercom stations that report audio level alarms.

7.5.1.8 CALL & EVENT LOGGING

All calls and events shall be logged to a log file. Log files shall be named and stored by date.

The current or historical log files shall be displayed on the screen or printed out on request. The system shall maintain log files for a minimum of six months. The system shall provide the operator with a warning prompt indicating the files should be backed up if required for a longer duration.

7.5.1.9 SYSTEM MAINTENANCE

The system shall be provided with a system configuration tool whereby system parameters may be set for individual intercom stations. All system parameters shall be downloaded from a Central station, and shall not require the opening of intercom points in order to change system parameters. Configuration should preferably be done with a HTML interface for each device.

The following maintenance parameters shall include but not be limited to:

(a) System Parameter Initialization;
(b) Intercom Station Parameters Configuration;
(c) Line Related Parameters Settings such as Station Type;
(d) Station Call Number Settings;
(e) Group Call Numbers Setting for Stations;
(f) Emergency Call Setting for Stations;
(g) Call Restriction Settings;
(h) Control Desk Group Settings;
(i) Configure Digital Switch Parameters;
(j) Print Pre-Defined Reports;
(k) Testing of Communication between PC and Digital Switch/s.

7.5.1.10 MULTIPLE OR SIMULTANEOUS CALLS

The system shall have programming capability for priority queuing so that problems can be assigned a higher precedence to pre-empt existing lower

7.5.1.11 SUPPRESSION OF CALLS

An operator shall be able to suppress calls. This shall be initiated in the event of nuisance calls from stations. The suppression of the call function shall only be available when enabled via a high-level password control allocated to a supervisor.
Once a station has been isolated calls initiated from the station shall not register at the operator stations.

7.5.1.12 FUTURE EXPANSION

The IP Intercom system shall be capable of being expanded for extended use within the total campus for future extensions. All upgrades to provide this service shall not affect the existing service as specified in this document or render the equipment, as specified, redundant in any form.

All system upgrades shall be configured using similar equipment and operate in the same manner in all respects. Any upgrades should cause minimal disturbance to the existing service.

7.6 INTERCOM STATIONS

Intercom stations shall consist of a vandal resistant, momentary action, call switch, speaker and microphone mounted into a flush mounted stainless steel plate.

7.6.1 INTERCOM UNITS

Intercom Units shall be designed/constructed/installed as follows:

(a) Front Plate, Grilles and Baffles:
(b) Speaker:
   • Mylar speaker with a 6 watt power rating;
(c) Microphone:
   • An Electret Type microphone with a minimum 36 dB dynamic range;
   • Adjustable Microphone Sensitivity.
(d) A tamper alarm separate to the call alarm to notify the respective operator station of an intercom unit’s removal;
(e) Call Button:
   • The call button is to be a robust, vandal resistant push button manufactured of stainless steel;
   • The call button shall activate a micro switch and bear against a solid shoulder, which resists knock through;
   • An internal neoprene gland seals the button to a minimum of IP65;
(f) Amplifier:
   • Build in 1-Watt amplifier with software adjustable gain.
(g) Cabling:
   • All connections must be made using RJ-45 connectors with a boot for the connector.
   • Intercom station electronic circuitry shall be optically isolated from the incoming data/audio bus.

7.7 DIGITAL AUDIO RECORDING SYSTEM

(a) A digital voice recording and playback system shall be supplied and installed as part of the Works;
(b) The central processor and associated peripherals shall support digital recording for a minimum of 32 channels without the requirement for additional central processors installed in each local area;
(c) The system shall support up to 32 channels of voice data information per central processor.
(d) Time and date stamping shall be automatically logged to all audio channels;
(e) The voice recording system central processor shall provide immediate access to, and recording of, voice inputs via an onboard storage medium to a minimum capacity of 30 days of on-line data. The storage should only be limited by the server HHD size.

(f) A CD-drive shall be installed as part of the central processor configuration for the archival of data;

(g) The audio recording system shall provide the following alarm conditions:
   - Recording medium capacity consumed by 80%;
   - When the hard disk reaches 90% of full capacity the system shall automatically over write the oldest dated data file. Access to the voice recording system shall be controlled by password authorization. A minimum of three levels of access rights shall be provided;

(h) The Intercom system supplied and installed, as part of these works shall be interfaced to the PSIM;

7.8 INTERCOM OPERATION

The intercom system shall be configured to provide the functionality as follows:

(a) In general, when a door intercom point is activated the intercom shall be answered from the relevant GUI operator station or Intercom GUI via a dedicated handset.

(b) The GUI terminal shall include a graphical display to connect and cancel intercom calls as elected.

(c) In the event of a door intercom point not being answered within the default time period of 30 seconds or the relevant GUI operator terminal being off-line the call shall automatically divert to the Central Control Station.
8 GENERAL INSTALLATION REQUIREMENTS

8.1 MAKING GOOD

(a) The Contractor will be responsible for making good in all trades, damage or disturbance to the buildings, installation, tarred surfaces, concrete surfaces which he or his employees may have caused damage in the course of the installation of equipment. The Contractor will be responsible for keeping the site tidy and shall remove from the site all rubble and litter resulting from his work.

8.2 INSTALLATION

(a) All installation costs shall be incorporated in the tender.
(b) A system schematic diagram shall be prepared and handed over to the Client as part of the Final Documentation.

8.3 PACKAGING, TRANSPORT, LOADING, STORAGE, SITE INFORMATION AND CONDITIONS

(a) The Contractor shall inform the Engineer of the Client, when the Equipment is ready for installation.
(b) The Contractor is advised to visit the site and acquaint himself with all local conditions pertaining to the execution of the installation before signing of the contract with the Client. No claims from the Contractor which may arise from insufficient knowledge of site access, type of site, labour conditions, establishment space, transport and loading/unloading facilities, power and water supply, etc., will be considered after submission of tenders.
(c) All Equipment shall be suitably packed for transporting to the site from the factory. The cost of packing and transport shall be included in the tender price. The Contractor shall be responsible for the loading, transport to the site, off-loading, storage rigging into position and security of the equipment on site or elsewhere as required. The regulations of the South African Government regarding shipping, customs tariff and inspection shall be complied with.

8.4 MATERIAL, EQUIPMENT AND WORKMANSHIP

(a) All material shall conform in respect of quality, manufacture, tests and performance, with the requirement of the South African Bureau of Standards or where no such standards exist, with the appropriate current specification of the British Standards Institution or the International Electro technical Commission.
(b) All material shall be new and of acceptable quality and suitable for the conditions on site. These conditions shall include weather conditions as well as conditions under which materials are installed, stored or used. Should the materials not be suitable for use under temporary site conditions then the Sub-Contractor shall at his own cost provide suitable protection until these unfavorable site conditions cease to exist.
(c) The Contractor shall, where requested to do so, submit samples of equipment and materials to the Engineer for his approval prior to installation. Samples may be retained in the Engineer's possession until the Contract is completed after which they will be returned.
(d) Locally manufactured equipment shall be used where possible and practical in preference to imported equipment. The Client in no way binds himself to assist the Sub-Contractor in obtaining import permits for imported equipment.
(e) The works shall be so installed as to provide ease of inspection, cleaning and maintenance.
(f) All artisans employed on site shall be competent in terms of the Regulations and Acts. All installations shall be carried out by qualified artisans or under the direct supervision of
qualified artisans. Installations (or part thereof) carried out by unskilled persons will be rejected.

(g) The Contract shall be executed to an acceptable standard and to the satisfaction of the Engineer. Should any workmanship, equipment or material not be to the satisfaction of the Engineer, it shall be rectified at the cost of the Contractor and all rejected materials shall be removed from site.

(h) If, in the opinion of the Engineer, any member of the Contractor’s staff is not competent to carry out the work to the required standard, then that person shall be removed from the project if so instructed by the Engineer.

The Contractor will not be Allowed to supply Equipment other than that Offered in His Tender without the Written Approval of the Client and Engineer.

8.5 PROGRAMME AND PROGRESS

(a) The programme for carrying out the works shall be submitted in detailed form covering all significant operations and shall be in the form of a Gant Chart (preferably in Microsoft Project Format). In addition, should the information be required in a particular format to suit project management requirements then such information shall be provided as part of this Contract.

(b) The Contractor shall liaise with all necessary parties (other Contractors, Sub-Contractors, Consultants, Equipment Suppliers, etc.) to ensure that the programme is as accurate and as realistic as possible.

(c) The Contractor shall submit the programme as soon as possible after award of the Contract but at the latest fourteen (14) days after award of the Contract.

(d) The programme shall list each scheduled item of equipment in the Contract and shall indicate periods for:
   • Preparation, Approval and Finalization of Manufacturing Drawings;
   • Ordering;
   • Manufacturing;
   • Inspection and Testing during Manufacture;
   • Delivery;
   • Installation;
   • Testing;
   • Commissioning.
   • The Contractor shall build into the programme, a period of two weeks, for approval of drawings by the Engineer.
   • The Contractor shall allocate to a senior member of his staff the duties of studying and evaluating the works in relation to the approved programme, of devising methods to overcome or prevent delays and of co-operating with the Engineer and other Contractors working on site. He shall report to the Engineer and draw his attention timeously to anything, which may cause a delay in the execution of the works.
   • The programme shall be updated as and when necessary to take account of changed circumstances.

8.6 CO-OPERATION WITH OTHER TRades

(a) The Contractor shall ascertain the extent of the work of other trades on site, which may affect, or be affected by the Contractor’s installation.

(b) The Contractor shall give all necessary assistance reasonably required to other trades to ensure that the work of such trades can be installed satisfactorily and without delay.

(c) The Contractor shall liaise with other trades working in close proximity to the work, covered by this specification, and shall assist in working out equipment and material positions to ensure that all trades can complete their work satisfactorily.
8.7 DRAWINGS

(a) The Engineer's drawings for the Contract shall be those issued at the times of tender together with any others issued to cover the variations to the Contract.

(b) As part of this Contract the Contractor shall provide the following Drawings:
   - Manufacturing and Installation Drawings:
     - The manufacturing and installation drawings ("shop drawings") shall provide all details of the components necessary for the manufacture and installation of the system in accordance with the specification.
     - Wiring Diagrams:
       - The wiring diagrams shall provide details of all the wiring associated with the installation.
       - The same drawing symbols and system shall be used, as used on the Engineer's Drawings.
     - Builder's Work Drawings:
       - All necessary builders’ work drawings, as described elsewhere in this specification, shall be provided as part of this Contract.
     - AS BUILT Drawings:
       - On completion of the installation, but before the plant is handed over; the Contractor shall provide a complete set of drawings showing the completed installation including wiring.
       - In addition to the drawings listed above, the Contractor shall provide all drawings necessary for the execution of the Contract and shall submit such general and detailed drawings of the components and apparatus, as the Engineer may require approving construction of the system.
       - Details and drawings of all major items of equipment, made by the Contractor or his suppliers, shall be submitted for approval without specific request from the Engineer.
       - All required drawings shall be submitted to an agreed programme to suit the construction of the system.
       - All drawings shall be clearly numbered or marked with the equipment item numbers, area references etc.

8.7.1 APPROVAL OF DRAWINGS

(a) The Contractor shall submit, for approval, copies of all abovementioned drawings prior to starting work or issue to other parties. Any work started (off site or on site) prior to receiving the Engineer's approval of drawings shall be at the Sub-Contractor's own risk.

(b) The Engineer may require from the Contractor further detailed drawings and/or calculations, which clarify features not adequately shown on the layout drawings. The request for additional details shall not be construed as extending the scope of this Contract or altering the programme.

(c) The Contractor shall submit three copies of each drawing to the Engineer for approval.

(d) The Engineer will return to the Contractor, within two weeks of their receipt by him one copy of each drawing marked 'APPROVED IN PRINCIPLE' or marked with any changes, which are necessary. The Contractor shall modify the details and drawings as required by the Engineer. The nature and date of each modification and a distinguishing symbol shall be added and the drawings shall be submitted again for approval.

(e) Alterations to drawings, by the Engineer, are not intended to change the scope of the work unless explicitly stated as doing so. Should any alterations, in the opinion of the Contractor, change the scope of work the Contractor shall notify the Engineer immediately of receipt of the altered drawings before any further drawing work or fabrication is carried out. Claims for a change of scope, made after performance of the work constituting the claimed change of scope of work will not be considered.

(f) The approval in principle of drawings by the Engineer shall not relieve the Contractor of any responsibility in terms of the Contract. The Engineer will check the drawings for design only.
and approval of the drawings, schedules and catalogues shall not be construed as a complete check.

(g) The Contractor shall be responsible for any discrepancies, errors or omissions in the drawings and other particulars supplied by him whether such drawings or particulars have been approved by the Engineer or not, provided that such discrepancies, errors or omissions are not due to inaccurate information or particulars furnished in writing to the Contractor.

(h) The Contractor shall provide, at his own expense, all copies of drawings required by him in the execution of the work and shall also, at his own expense, supply to the Engineer such drawings and copies thereof as are provided for in the specification.

(i) On completion of the installation, but before final handover, the Contractor shall provide three high quality paper prints of each of the Contract drawings showing the system as fixed. These Drawings will be folded and included in the AS BUILT Documentation. The Drawings shall include, but not be limited to:
   - Complete 1:50 Scale Layouts of Plant Rooms;
   - Complete 1:100 Scale Drawings of the Whole Installation;
   - Detailed Drawings of All Items of Plant;
   - Electrical Layouts and Wiring Diagrams;
   - Details of Any Other Items Requested by the Engineer.
   - The drawings shall be sufficient in detail to enable the Client's staff to maintain, dismantle, reassemble and adjust any part of the works.

8.8 INFORMATION REQUIRED

(a) Tenderers shall furnish detailed descriptions and illustrations of the equipment offered and shall complete the questionnaire following this specification. This includes drawings of the switchboard layouts and control diagrams.

(b) Failure to submit any of the information asked for may disqualify the tender.

8.9 TOOLS AND EQUIPMENT

(a) Unless otherwise specified, the Contractor shall provide all tools, materials, scaffolding, power, water, etc., necessary for the proper and efficient execution of the work covered by this specification.

(b) No extra payment will be made for plant, equipment, materials required by the Contractor to complete the work.

(c) The Contractor shall provide all rigging, cranes, lifting, equipment, etc., necessary to execute the works.

8.10 STORAGE OF EQUIPMENT AND MATERIALS

(a) The Contractor shall ensure that all stored materials and equipment are safely stacked and that stacking does not damage them.

(b) The Contractor shall ensure that stored materials and equipment do not overload the structure or floor construction.

(c) The storage of combustible materials on site shall be kept to a minimum. The Contractor shall be responsible for ensuring that such combustible materials are safely stored. Suitable fire fighting equipment shall be provided by the Contractor, who shall further ensure that staff capable of using the equipment is at hand.
8.11 LOCATION OF EQUIPMENT

(a) The Contractor shall check on doorways, passages, openings, lifts, etc. provided and shall ensure that all equipment offered can be moved through them to its final position. If necessary, equipment shall be ordered in a partially dismantled condition so that it is suitable for moving through the restricted openings or areas of restricted height or areas of restricted load.

8.12 MAINTENANCE TOOLS

(a) The Contractor shall provide one set of all special tools, panel keys, etc., required for testing, maintaining and operating of all items of equipment.
(b) Duplicate keys shall be provided for all control panels, instrument locks, etc.

8.13 AVAILABILITY OF SPARES

(a) Spares and replacement parts shall be readily available in the Republic of South Africa and a guarantee of availability for a period of ten years shall be furnished.
(b) The Contractor shall submit a priced schedule of recommended spare parts, which should be carried on site.

8.14 INSTRUCTION OF OPERATOR

(a) On completion of all tests, to the satisfaction of the Engineer, the Contractor shall continue to be responsible for the complete operation and maintenance of the plant for a period of three weeks during which time instructions shall be given to the Client's staff of the proper operation and maintenance of the plant, until he is fully conversant with the equipment and the handling thereof. The cost for such training shall be included in the tender price.
(b) The operation and maintenance of the plant, for the duration of the instruction period, shall not in any way relieve the Contractor of his responsibility under the terms of the Contract.
(c) Three copies of a Maintenance, Fault-Locating and Operating Manual are to be handed over to the Client’s representatives on site together with the Drawings specified above.

8.15 OPERATING AND MAINTENANCE MANUALS

(a) The Contractor shall provide three (3) copies of the Operating and Maintenance Manuals.
(b) The Contractor shall submit, for approval to the Engineer, four (4) weeks before completion of the installation, one (1) copy of the maintenance and operating manuals for the system supplied.
(c) The Engineer will return these to the Contractor, within ten (10) working days of their receipt by him, marked with all changes, which are necessary.
(d) The Contractor shall modify the manuals, as required by the Engineer and submit to the Engineer, within ten (10) working days, one (1) revised copy of the manuals. On completion of the installation, but before the plant is handed over to the Client; the Contractor shall provide three (3) copies of the Final Operating and Maintenance Manuals for the system supplied. The manuals shall be bound in book form with hard plastic covers to withstand constant use.
(e) The Manuals shall be Properly Indexed to Facilitate Easy Reference.
(f) The Manuals shall Include:
   • A List of Recommended Servicing Tools and Specialist Equipment;
   • A List of Spares to be Supplied by the Contractor to Cover the Period of Warranty. The Spares to be Supplied during the Warranty Period will However not be Limited to the Listed Items;
A Priced List of Recommended Spares Necessary for a Period of four (4) Years of Operation;
Exploded Drawings for detailed spares list from which every item of Every Piece of Equipment can be Positively Identified for Ordering Replacements;
A List giving the Name and Address of the Local Agent for each Item of Equipment;
A List giving the Name and Address of the Manufacturer of Each Item of Equipment;
Originals of All Test Certificates Obtained with the System;
A Preventative Maintenance Programme for All Equipment;
Operating Instructions for Each Item of Equipment;
Performance Data and/or Characteristic Curves;
Commissioning Data;
Record Drawings.
### 9 APPENDIX A – TECHNICAL SUPPORT DOCUMENTATION

#### 9.1 WORKSTATION ICONS

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Door Secure Icon" /></td>
<td>DOOR SECURE</td>
</tr>
<tr>
<td><img src="image2" alt="Door Un-Secure Icon" /></td>
<td>DOOR UN-SECURE</td>
</tr>
<tr>
<td><img src="image3" alt="Door Fault Icon" /></td>
<td>DOOR FAULT</td>
</tr>
<tr>
<td><img src="image4" alt="Door Interlocked Icon" /></td>
<td>DOOR INTERLOCKED</td>
</tr>
<tr>
<td><img src="image5" alt="Door Excluded from Group Icon" /></td>
<td>DOOR EXCLUDED FROM GROUP</td>
</tr>
<tr>
<td><img src="image6" alt="Door Included in Group Icon" /></td>
<td>DOOR INCLUDED IN GROUP</td>
</tr>
<tr>
<td><img src="image7" alt="Door Emergency Released Icon" /></td>
<td>DOOR EMERGENCY RELEASED</td>
</tr>
<tr>
<td><img src="image8" alt="Motorised Door Secure Icon" /></td>
<td>MOTORISED DOOR SECURE</td>
</tr>
<tr>
<td><img src="image9" alt="Motorised Door Open Icon" /></td>
<td>MOTORISED DOOR OPEN</td>
</tr>
<tr>
<td><img src="image10" alt="Roller Shutter Secure Icon" /></td>
<td>ROLLER SHUTTER SECURE</td>
</tr>
<tr>
<td><img src="image11" alt="Roller Shutter Un-Secure Icon" /></td>
<td>ROLLER SHUTTER UN-SECURE</td>
</tr>
<tr>
<td><img src="image12" alt="DPS Secure Icon" /></td>
<td>DPS SECURE</td>
</tr>
<tr>
<td><img src="image13" alt="DPS Un-Secure Icon" /></td>
<td>DPS UN-SECURE</td>
</tr>
<tr>
<td><img src="image14" alt="Fence Zone Healthy Icon" /></td>
<td>FENCE ZONE HEALTHY</td>
</tr>
<tr>
<td><img src="image15" alt="Fence Zone Alarm Icon" /></td>
<td>FENCE ZONE ALARM</td>
</tr>
</tbody>
</table>

- CAMERA DE-SELECTED
- CAMERA SELECTED
- AUDIO EVESDROP ON
- PS UN-SELECTED
- PA SELECTED
- AUDIO CHANNEL ON
- AUDIO CHANNEL OFF
- AUDIO CHANNEL CALLING
- AUDIO CHANNEL FAULT
- AUDIO EVESDROP OFF
- PANIC BUTTON NON ACTIVE
- PANIC BUTTON ACTIVE
- PANIC BUTTON ACKNOWLEDGE
- UPS HEALTHY
- UPS FAILURE
CELL LIGHT OFF

CELL LIGHT ON

PC WORKSTATION HEALTHY

PC WORKSTATION FAILURE

MOTION DETECTION HEALTHY

MOTION DETECTION ALARM

MOTION DETECTION ALARM ACKNOWLEDGE

DAY ROOM BAY LIGHTS OFF

DAY ROOM BAY LIGHTS ON

LIGHT GROUP NOT SELECTED

LIGHT GROUP NOT SELECTED

GROUP PROGRAM MODE IS NOT SELECTED

GROUP PROGRAM MODE IS SELECTED

DOOR GROUP OPERATE NOT SELECTED

DOOR GROUP OPERATE SELECTED

EMERGENCY GROUP OPERATE NOT SELECTED

EMERGENCY GROUP OPERATE SELECTED

AIR PRESSURE HEALTHY

AIR PRESSURE LOW

COMPRESSOR HEALTHY

COMPRESSOR FAILURE

VEHICLE LOOP DETECTOR IN-ACTIVE

VEHICLE LOOP DETECTOR ACTIVE
This page must be completed and returned with the returnable portion of the tender document. Failure to do so will result in immediate disqualification of the tender.

10 APPENDIX B – SOFTWARE SYSTEMS

10.1 SCHEDULE OF SOFTWARE OFFERED

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th>Is the software fully compliant?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Are all settings, interfaces, etc. modifiable by the user and fully parameter driven?</td>
<td>Yes</td>
</tr>
<tr>
<td>2.</td>
<td>Is any service, configuration change, etc. accessible and can it be done in no more than 2 mouse clicks?</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Are all protocols and interfaces interchangeable?</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Is all interconnectivity totally transparent?</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Are all interfaces fully defined in the user manual?</td>
<td></td>
</tr>
</tbody>
</table>

DECLARATION

I, THE UNDERSIGNED (name) ……………………………………………………………………….hereby certify that the information furnished in Appendix D above is correct.

I accept that the CLIENT as representative of the Government of the Republic of South Africa may act against me should this declaration prove to be false.

Signature: ............................................ Date: ................................................

Identity number: ………………………………………………………………………………………

Position: ………………………………………………………………………………………………

Name of Tenderer: ………………………………………………………………………………………

This page must be completed and returned with the returnable portion of the tender document. Failure to do so will result in immediate disqualification of the tender.
## APPENDIX C – SCHEDULE OF EQUIPMENT OFFERED

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Yes / No</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 DOOR CONTROLLERS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Manufacturer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Country of Origin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Country of Manufacture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Supplier in South Africa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Does the system comply fully with the specification in full.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5.1</td>
<td>Make</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5.2</td>
<td>Model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the System does not fully comply please indicate exactly where:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Yes / No</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2 BREAK GLASS UNITS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Manufacturer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Country of Origin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3</td>
<td>Country of Manufacture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td>Supplier in South Africa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5</td>
<td>Does the system comply fully with the specification in full.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.1</td>
<td>Make</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.2</td>
<td>Model</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the System does not fully comply please indicate exactly where:
### 3 LIGHTNING & SURGE PROTECTION

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>3.2</td>
<td>Country of Origin</td>
</tr>
<tr>
<td>3.3</td>
<td>Country of Manufacture</td>
</tr>
<tr>
<td>3.4</td>
<td>Supplier in South Africa</td>
</tr>
<tr>
<td>3.5</td>
<td>Does the system comply fully with the specification in full.</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Make</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Model</td>
</tr>
</tbody>
</table>

If the System does not fully comply please indicate exactly where:

### 4 BIOMETRIC READERS

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>4.2</td>
<td>Country of Origin</td>
</tr>
<tr>
<td>4.3</td>
<td>Country of Manufacture</td>
</tr>
<tr>
<td>4.4</td>
<td>Supplier in South Africa</td>
</tr>
<tr>
<td>4.5</td>
<td>Does the system comply fully with the specification in full.</td>
</tr>
<tr>
<td>4.5.1</td>
<td>Make</td>
</tr>
<tr>
<td>4.5.2</td>
<td>Model</td>
</tr>
</tbody>
</table>

If the System does not fully comply please indicate exactly where:
## 5 ELECTROMECHANICAL LOCKS

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>5.2</td>
<td>Country of Origin</td>
</tr>
<tr>
<td>5.3</td>
<td>Country of Manufacture</td>
</tr>
<tr>
<td>5.4</td>
<td>Supplier in South Africa</td>
</tr>
<tr>
<td>5.5</td>
<td>Does the system comply fully with the specification in full.</td>
</tr>
<tr>
<td>5.5.1</td>
<td>Make</td>
</tr>
<tr>
<td>5.5.2</td>
<td>Model</td>
</tr>
</tbody>
</table>

If the System does not fully comply please indicate exactly where:

---

### DECLARATION

I, THE UNDERSIGNED (name) ……………………………………………………………………….hereby certify that the information furnished in Appendix D above is correct.

I accept that the CLIENT as representative of the Government of the Republic of South Africa may act against me should this declaration prove to be false.

**Signature:** ……………………………. **Date:** ………………………………………

**Identity number:** ……………………………………………………………………………

**Position:** …………………………………………………………………………………

**Name of Tenderer:** ……………………………………………………………………….

---

This page must be completed and returned with the returnable portion of the tender document. Failure to do so will result in immediate disqualification of the tender.
APPENDIX D – TECHNICAL DELIVERABLES

The following documentation must be included in the submission of the tender document. Failure to do so will result in immediate disqualification.

**Previous Experience**
The tenderer must include a list of relevant previous experience in the industry. The scoring will be done in accordance with the scoring criteria of EDC Services, which will be provided to the tenderer as part of the Tender Documentation Package.

**Contactable References**
The tenderer must include a list of relevant contactable references where similar installations was concluded by the tenderer, or where similar installations are still in progress. The scoring will be done in accordance with the scoring criteria of EDC Services, which will be provided to the tenderer as part of the Tender Documentation Package.

**Curriculum Virtue of relevant Employees**
The tenderer must include the CV's of all relevant employees as proof that they are qualified and capable to perform all relevant tasks at hand. The scoring will be done in accordance with the scoring criteria of EDC Services, which will be provided to the tenderer as part of the Tender Documentation Package.

**Technical Data Sheets**
The tenderer must complete and return Appendix A as well as Appendix B of the GENERAL SPECIFICATION FOR THE SMOKE DETECTION PORTION OF THE INTEGRATED SECURITY SYSTEM. A technical data sheet of each equipment the tenderer purposes must be included in the deliverables.

**Method Statement**
The tenderer must include a detailed method statement that clearly specify how the project will be conducted. This is to determine that the tenderer understand what is expected from him/her during the installation of the project. The scoring will be done in accordance with the scoring criteria of EDC Services, which will be provided to the tenderer as part of the Tender Documentation Package.

**Program**
The tenderer must include a detailed program that will be followed for the duration of the project. The tenderer must clearly indicate, to the best of his/her knowledge the amount of time that is reasonable to complete the project. It must be taken into account that the work will only be conducted after hours and weekend due to the nature of the site. The scoring will be done in accordance with the scoring criteria of EDC Services, which will be provided to the tenderer as part of the Tender Documentation Package.

**Socio-Economic**
The tenderer must include a clear Socio-Economic plan for this project. The scoring will be done in accordance with the scoring criteria of EDC Services, which will be provided to the tenderer as part of the Tender Documentation Package.