



Shared
ServicesBC

ACCOMMODATION AND REAL ESTATE SERVICES (ARES)

SECURITY SYSTEM SPECIFICATIONS

Security System Specifications

Accommodation and Real Estate Services (ARES)

Table of Contents

1.	GENERAL.....	3
1.1.	LICENCES, APPROVALS, PERMITS, & STANDARDS	3
1.2.	GENERAL CONDITIONS	3
1.3.	DOCUMENTATION	4
1.4.	TRAINING	4
1.5.	WIRING & INSTALLATION	4
2.	SYSTEMS.....	5
2.1.	INTRUSION ALARM SYSTEM.....	5
2.2.	PANIC ALARMS	9
2.3.	REMOTE DOOR CONTROL	10
2.4.	REMOTE DOOR RELEASE	10
2.5.	ACCESS CONTROL SYSTEMS	10
2.6.	AUDIO INTERCOM	12
2.7.	VIDEO INTERCOM.....	12
2.8.	CLOSED CIRCUIT TELEVISION (CCTV) SYSTEMS.....	12
2.9.	PERIMETER ALARM SYSTEMS	14

1. GENERAL

1.1. LICENCES, APPROVALS, PERMITS, & STANDARDS

- 1.1.1. The contractor must be provincially licensed by the Security Programs Division of the Ministry of Public Safety and Solicitor General to install alarms (PISA Act - ASR1).
- 1.1.2. The contractor shall be responsible for all permits, licenses, inspections and related fees.
- 1.1.3. The installation and commissioning of electronic security systems shall be by qualified alarm service technicians who shall be licensed by the Security Programs Division of the Ministry of the Solicitor General.
- 1.1.4. For the purposes of these specifications ARES shall mean ARES or their appointed representative WSI (Workplace Solutions Incorporated).
- 1.1.5. The contractor shall not sub-contract any portion of the installation without prior approval of WSI.

1.2. GENERAL CONDITIONS

- 1.2.1. The contractor shall be fully trained and factory certified on all security systems as required by this document.
- 1.2.2. WSI will have complete control of the operation of the system(s) while the building is occupied by ARES or its tenants.
- 1.2.3. All equipment shall remain the sole property of WSI and the installing company will not retain ownership or control of the system.
- 1.2.4. All hardware and software (including the Windows operating system) required to make programming changes to the system(s) shall be included with the system. Hard copies of all software licenses shall be provided.
- 1.2.5. Each system shall have sufficient power supply to operate the system and the manufacturers' recommended power for the system shall be less than 80% of the power supply rated power output.
- 1.2.6. All systems shall include sufficient back up power supply to operate all devices simultaneously without drawing more than 80% of the capacity of the power supply. The back up power system shall have sufficient capacity to operate the entire system for a minimum of 24 hours under normal operating conditions. (All batteries to be minimum 7 amp hour)
- 1.2.7. All systems shall be configured to be managed onsite. Certain systems may require the ability to be remotely controlled and configured (as specifically identified on a site by site basis).
- 1.2.8. All exceptions to these standards and specifications (including the determination of equivalencies) shall be at the sole discretion of WSI.
- 1.2.9. All systems to be on a separate, standalone network and will not be connected to the SPAN BC government network.

1.3. DOCUMENTATION

1.3.1. The contractor shall provide the following documentation to WSI:

- .1 All user manuals
- .2 All installation manuals
- .3 As-built drawings showing location of all devices, controls, demark connection, panels and keypads
- .4 All zones shall be clearly identified on the drawings
- .5 Electrical panel circuit breaker shall be clearly identified and noted on both the panel cover and as-built drawings
- .6 A printout of the monitoring company activity report that verifies full system testing
- .7 Device verification sign-off sheets
- .8 Manufacturer's cut sheets for all devices
- .9 All forms as supplied by WSI
- .10 Electrical inspection permit and report

1.4. TRAINING

- 1.4.1. Training shall be provided for each individual system as required by this document. Training shall include a minimum of 2 hours per system and shall be conducted at a time that is mutually agreeable to both the contractor and WSI.
- 1.4.2. Contractor shall provide WSI with a training attendance sign-off sheet. This sheet shall identify the site, time and date as well as a listing of all those in attendance.

1.5. WIRING & INSTALLATION

- 1.5.1. Unless otherwise specified, ARES security systems do not require conduit – except in exposed or exterior locations. All wiring must comply with all applicable codes and meet all standards as required by the local AHJ (Authorities Having Jurisdiction).
- 1.5.2. All security control panels shall be located in a secure, accessible location within the protected space (i.e. – panels and equipment shall not be mounted in electrical or data rooms that are not within the protected space).
- 1.5.3. All cable and equipment supplied, and all installation methods used, shall be as specified by the equipment manufacturer.
- 1.5.4. All systems shall be wired using cable acceptable to the authority having jurisdiction for the building.
- 1.5.5. All CCTV coaxial cable connections shall be made using crimped or pre-manufactured connectors only.
- 1.5.6. No splices shall be permitted in the wiring except where a connection is made to a device. All connections shall be made using "B" clips, stakons or approved equivalent (no marrettes).

- 1.5.7. All wiring shall be concealed unless otherwise authorized by ARES.
- 1.5.8. All cables shall be permanently identified and listed on as-built drawings as follows:
 - .1 Cable number
 - .2 Source
 - .3 Destination
- 1.5.9. Electrical panel circuit number shall be clearly identified on all system panels.
- 1.5.10. All work shall be installed in a neat and workmanlike manner. The contractor is responsible for clean up and disposal of all garbage and debris caused as a result of their work.
- 1.5.11. Wiring penetrating any horizontal or vertical assembly required to have a fire-resistance rating shall be in accordance with the local AHJ. Conduits or cables shall be tightly fitted and fire stopped where necessary to maintain fire rating.
- 1.5.12. Contractor shall repair at no cost to the Owner, any equipment or structures damaged by the execution of their contract to its original condition.

2. SYSTEMS

2.1. INTRUSION ALARM SYSTEM

2.1.1. General

- 2.1.1.1. The protected space shall be provided with a complete intrusion alarm system. Intrusion protection shall be provided by way of door contact switches, glass break detectors and motion sensors as required. The intrusion alarm system is designed to detect unauthorized entry into protected spaces. The system shall conform to the requirements of this document.
- 2.1.1.2. The intrusion alarm system may be broken into separate partitions (areas).
- 2.1.1.3. The intrusion alarm control panel shall have a sufficient number of zone inputs so that each device shall be connected to a single zone (double doors may be grouped as a single zone).
- 2.1.1.4. Home-run all devices to the alarm panel - do not gang or group devices unless otherwise authorized by WSI.
- 2.1.1.5. The system shall have the capacity to provide one access code per person for the full occupancy of the protected space.
- 2.1.1.6. When partitioned, each partition of the intrusion alarm system will have as a minimum the following devices:
 - .1 Full LCD keypad
 - .2 Door contact
 - .3 Motion Detector
- 2.1.1.7. The panel make and model shall be approved in advance by WSI. The panel shall be non-proprietary (i.e. – available to all alarm contractors.)

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.1.1.8. The panel power supply shall be a minimum 37 VA. It shall be hard-wired to a dedicated, non-switched source (i.e. no plug-in type transformers) and the circuit # be clearly identified on both the electrical panel directory and on the alarm panel.
- 2.1.1.9. Battery back up shall be gel-cell type, minimum 7 amp/hour. Battery installation date shall be marked on the battery and panel cover.
- 2.1.1.10. All devices (including the panel) shall be supervised with tamper switches and end of line resistors.
- 2.1.1.11. EOL devices shall be installed at the device – not in the panel.
- 2.1.1.12. A copy of the zone descriptors shall be left inside the alarm panel.
- 2.1.1.13. Standard of Acceptance:
DSC PC 1864 or 4020 series (most current versions)
- 2.1.2. Programming
 - 2.1.2.1. The contractor shall be responsible for all programming of the alarm system. This includes all user codes; all zone definitions and establishing a connection to the WSI monitoring station.
 - 2.1.2.2. WSI shall supply the contractor with all access codes and phone numbers to be programmed into the alarm system.
 - 2.1.2.3. The panel shall be programmed in SIA format.
 - 2.1.2.4. The contractor shall program the following:
 - .1 User code required to bypass zones
 - .2 Daily test transmission (early morning – not on the hour)
 - .3 Bell time-out shall be set at 4 minutes
 - .4 Home-away enabled
 - .5 Disable reporting of partition opening/closing. All reporting is to be by user only
 - .6 All panels shall be programmed to auto-arm at 23:00 daily
 - 2.1.2.5. The contractor shall not install a contractor's lockout enable and shall not program Forced Arming or Auto-Disarming without prior approval from WSI.
 - 2.1.2.6. Upon completion of programming the installer shall initiate an upload of the panel programming to Safelink (WSI authorized monitoring agent).
 - 2.1.2.7. The contractor shall not access the system either physically or by modem without WSI approval.
- 2.1.3. Monitoring
 - 2.1.3.1. WSI retains the right to monitor their alarm systems in the manner of their choosing and will not be locked into any other monitoring arrangements.

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.1.3.2. Monitoring is normally arranged by WSI.
- 2.1.3.3. All telephone jacks used for alarm/security systems shall be wired to USOC RJ31 and shall be installed to industry standards.
- 2.1.3.4. WSI shall issue all phone numbers for monitoring and downloading. All intrusion alarm systems shall be connected to analogue telephone lines (no voice over internet {VOIP} lines).
- 2.1.3.5. All position eight (8) jacks shall be installed with a tamper loop, ahead of the demark block.
- 2.1.4. Keypads
 - 2.1.4.1. No global keypads - each partition will have its own keypad
 - 2.1.4.2. All keypads shall be LCD alpha (full English) type (unless otherwise specified)
 - 2.1.4.3. List all zones on the keypad in a clear and legible manner
 - 2.1.4.4. All keypad panic buttons shall be disabled
 - 2.1.4.5. All keypads to be set up for "Quick Arming" ("X-0")
 - 2.1.4.6. All keypads to be installed at 1.372m (54") above finished floor.
- 2.1.5. Sirens/Strobes
 - 2.1.5.1. The system shall include sufficient interior alarm sirens to provide an audible alarm warning throughout the protected space; more than one siren may be required. The contractor shall supply any additional sirens should the space require them to meet the above criterion. (Interior sirens to be minimum 15 watt).
 - 2.1.5.2. All sirens and strobes to be on an isolated power supply.
 - 2.1.5.3. All systems shall be programmed for 4 minute bell duration.
 - 2.1.5.4. An exterior strobe (blue) shall be installed for all ground floor systems, location to be decided in consultation with WSI.
 - 2.1.5.5. The strobe shall be latched so that the panel must be reset to turn it off. (The strobe will provide staff with a warning that the alarm system has been activated.)
 - 2.1.5.6. An audible warning shall be provided when the system is armed or during the exit delay period. The armed warning tone shall be different from the alarm siren sound and shall be audible throughout the protected space. This may require additional sirens or tone devices to be added throughout the protected space so that all staff can hear the alert.
 - 2.1.5.7. Standard of Acceptance:
Interior Sirens – Honeywell WAVE-F, Ademco 746
Exterior strobe/siren (blue) - Amseco SSX 51SB, ATW PR-DOBERMAN
- 2.1.6. Motion Detectors

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.1.6.1. Motion detectors shall only be dual technology type (PIR and microwave).
- 2.1.6.2. All motion detectors shall be field-adjusted as per manufacturer's specifications for full coverage pattern of the protected spaces.
- 2.1.6.3. All motion detectors shall have LED's disabled after initial testing is done.
- 2.1.6.4. Standard of Acceptance:
Optex MX, DSC Force II, Honeywell DT series
- 2.1.7. Glass Break Devices
 - 2.1.7.1. All devices shall be installed and field-adjusted as per manufacturer's specs.
 - 2.1.7.2. Standard of Acceptance:
GE SR-5815NT, Honeywell FG730
- 2.1.8. Door/Window Contacts
 - 2.1.8.1. Every door which leads to the protected space shall be fitted with a door contact switch.
 - 2.1.8.2. All grade level or easily accessible opening windows shall be equipped with a contact.
 - 2.1.8.3. All door contacts shall be installed at the top of the door, opposite the hinge side of the door.
 - 2.1.8.4. All door and window contacts must be "wide gap" type.
 - 2.1.8.5. All door and window contacts must be concealed unless otherwise directed. If installed in wood or similar material, allow for expansion. Fill all voids with RTV silicone or equivalent.
 - 2.1.8.6. Standard of Acceptance:
GE Sen1078 series, Amseco AMS-25A/B
Overhead doors: GE SEN2200, Amseco ODC-59A/B
- 2.1.9. Cellemetry Back-Up
 - 2.1.9.1. Where a cellemetry back-up unit is installed it must be equipped with its own power supply, which is sized to meet the power requirements of the cellemetry unit.
 - 2.1.9.2. The cellemetry power supply shall be hard wired to a dedicated, non-switched source (i.e. no plug-in type transformers) and the circuit # clearly identified on both the electrical panel directory and on the alarm panel.
 - 2.1.9.3. A separate back-up battery for the cellemetry unit must also be supplied. Battery back up shall be gel-cell type, minimum 7-amp/hour. Battery installation date shall be marked on the battery and panel cover.
 - 2.1.9.4. Cellemetry panel to be placed in location that is physically and visually separated from the main alarm panel (so that intruders cannot readily find the cellemetry panel to disable it).

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.1.9.5. The cellemetry panel shall monitor Burglary (a separate zone coded as such) and TLM (telephone line monitoring). These zones shall be coded and identified as coming from the cellemetry panel.
- 2.1.9.6. Standard of Acceptance: Unit must be digital
Uplinks UPL DigiCell Anynet model 19-25133-070 (1-888-987-5465)
<http://www.uplink.com>
DSC GSM Alarm Communicator MODEL GS3055-I <http://www.dsc.com>

2.2. PANIC ALARMS

2.2.1. General

- 2.2.1.1. Panic alarms shall be activated by a hardwired recessed push buttons which have to be manually reset after activation.
- 2.2.1.2. All panic buttons shall be clearly identified by a label (Brother P2000 or equivalent).
- 2.2.1.3. All panic buttons located on movable furniture shall be connected using an RJ 12 wall jack and a telephone patch cord to the jack. The wall jack shall be clearly identified by a label marked "Panic System" (Brother P2000 or equivalent).

2.2.2. Local Response Systems (Not monitored)

- 2.2.2.1. Unless specified, the panic alarm system shall be a separate, standalone system and will not be monitored.
- 2.2.2.2. Local panic systems will not be integrated into the main intrusion alarm panel.
- 2.2.2.3. When the panic alarm push button is pressed, a flashing light and chime (or other unique audible signal) shall sound in a remote designated area (signal should not be within sight or hearing of push button location).
- 2.2.2.4. Where multiple panic alarm locations are provided, a standalone panel shall be installed.
- 2.2.2.5. Each standalone panic alarm panel will be controlled by an LED keypad that will clearly identify the location of each panic button. If more than 16 panic buttons are required then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panels.
- 2.2.2.6. Make and model of panic button shall be decided in consultation with WSI representative.
- 2.2.2.7. Standard of Acceptance:
Multi-zone non-monitored panel: DSC 5010 or 4020
Panic button: Potter HUB-M (non-latching), GE Sentrol 3045 (non-latching LED)

2.2.3. Monitored Panic Alarm Systems

- 2.2.3.1. As per above specifications except that each panic button shall be connected to the main intrusion alarm system panel and each panic button shall be identified as an individual zone. If more than 16 panic buttons are required

then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panels.

- 2.2.3.2. WSI is to be consulted as to whether or not monitored panic buttons will also report locally. (Note that most monitored panic alarms do not report locally - either audibly or with a strobe).

2.2.4. Wireless Panic Alarm Systems

- 2.2.4.1. Wireless panic alarms shall only be installed at the direction of ARES.
- 2.2.4.2. All wireless panic alarms must be tested throughout the entire protected area so as to ensure that the panic buttons work in all locations
- 2.2.4.3. Standard of Acceptance:
Visonic MCT 201, MCT 124; Honeywell 5802 MN2

2.3. REMOTE DOOR CONTROL

- 2.3.1. Designated door(s) will have a selector switch that will enable the door to be remotely locked or unlocked during business hours.
- 2.3.2. The selector switch to be interfaced with the card access system.
- 2.3.3. The selector switch will be clearly labeled "Open" and "Locked".
- 2.3.4. Standard of Acceptance:
Camden CM 190/4

2.4. REMOTE DOOR RELEASE

- 2.4.1. Designated door(s) will have a push button that will enable the door to be remotely released during business hours.
- 2.4.2. The push button is to be interfaced with the card access system.
- 2.4.3. The push button will be clearly labeled as to which door is controlled.
- 2.4.4. Standard of Acceptance:
Camden CM 9280

2.5. ACCESS CONTROL SYSTEMS

2.5.1. General

- 2.5.1.1. The protected space shall be provided with an access control system. Card readers and electric locking devices shall be installed at all designated entry doors to the protected space, including stairwell doors at points of public access. If an elevator is used to directly access the protected space, the card access system shall also be used to control the movement of the elevator on a floor by floor basis.
- 2.5.1.2. The system shall be expandable to allow for a minimum of 20% additional card readers.

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.5.1.3. The system shall have the capacity of either: one access card for every 10m² of the protected space, or the number of cards immediately required by the tenant plus 20%.
- 2.5.1.4. 26 bit HID Proximity cards or FOB's (or card formats of WSI choice) shall be provided.
- 2.5.1.5. The access system may be interfaced with the intrusion alarm system, so that access cards can disarm the intrusion alarm system. The access system shall disarm by first user in (not auto-disarm).
- 2.5.1.6. The card system shall be programmable and shall allow users to determine which doors can be accessed and at what time of day
- 2.5.1.7. Every door that has a card reader and electric locking device shall also have a door contact and request to exit motion sensor (not a push button) in order to provide door held open/door forced open functions.
- 2.5.1.8. The access system shall record all door held open/forced open events and shall be capable of providing an audible alarm and a voltage or dry contact output for these conditions.
- 2.5.1.9. The system shall include all computer hardware, peripherals and software necessary to operate and record all system event history on the computer's hard drive. The system shall be capable of generating a variety of historical reports which can be outputted to the computer screen and/or to a printer. The system shall allow the user to make changes to all system parameters including access card and schedule changes. New computer hardware and peripherals shall be supplied as part of the system and shall meet or exceed the manufacturer's requirements.
- 2.5.1.10. The access system shall not be dependent on the computer for its operation. That is, the access control panels shall be able to continue to operate 24 hours a day, 7 days a week without any degradation in the operation of the system even if the computer hardware and software are completely disconnected from the access control panels.
- 2.5.1.11. This shall include a minimum of three (3) workstation licenses.
- 2.5.1.12. All readers to be installed at .9144m (36") above finished floor.
- 2.5.1.13. Standard of Acceptance:
Kantech Entra-Pass (most current version), HID readers
- 2.5.2. Electric Strikes
 - 2.5.2.1. Unless otherwise specified, electric strikes are the only acceptable electric locking devices. All locking devices must meet the building, fire and electrical code requirements of all AHJ.
 - 2.5.2.2. Unless otherwise directed electric strikes shall fail "secure."
 - 2.5.2.3. All electric strikes shall be 12/24 volt dc.

- 2.5.2.4. Standard of Acceptance:
Rutherford, Securitron, Folger Adam

2.6. AUDIO INTERCOM

- 2.6.1. The audio intercom unit will be installed adjacent to the designated entry door at 1.525 m (5 ft). The base station will be mounted in a location of the client's choosing.
- 2.6.2. The client may elect to have the intercom interfaced with the entry door controls so that they can remotely release the door. The contractor is responsible for all interfacing between the various systems.
- 2.6.3. Standard of Acceptance:
System - Aiphone IE Series, Exterior door station - IE-SS

2.7. VIDEO INTERCOM

- 2.7.1. The video intercom unit will be installed adjacent to the designated entry door at 1.525 m (5 ft). The base station will be mounted in a location of the client's choosing.
- 2.7.2. The client may elect to have the video intercom interfaced with the entry door controls so that they can remotely release the door. The contractor is responsible for all interfacing between the various systems.
- 2.7.3. Standard of Acceptance:
Aiphone MK-1GD (B+W), KC Series (colour), Exterior door station – MK-DVF (B+W), KB-DVF (colour)

2.8. CLOSED CIRCUIT TELEVISION (CCTV) SYSTEMS

2.8.1. General

- 2.8.1.1. CCTV systems shall not violate the rights of privacy and other legal rights of persons under observation. In particular, signs shall be provided where routine surveillance is conducted, advising that the space is under electronic surveillance. Signage should be in the languages spoken in the area. Cameras shall not be installed where there is a reasonable expectation of privacy; i.e. washrooms, change-rooms or other similar spaces. Refer to the following web site: http://www.mser.gov.bc.ca/foi_pop/main/video_security.htm
- 2.8.1.2. CCTV system to be on separate, standalone network and will not be connected to the government network.
- 2.8.1.3. The CCTV system shall include all equipment necessary to give a fully functioning system.
- 2.8.1.4. Closed circuit television systems shall be professionally designed.

2.8.2. Cameras

- 2.8.2.1. All cameras shall be powered from an approved camera manufacturer power supply. All connections shall be crimped.
- 2.8.2.2. The camera shall be pre-packaged vandal resistant domes. The units must be available in both indoor and outdoor versions.

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.8.2.3. The camera housing must be constructed a high-impact polycarbonate bubble. Tamper-resistant security hardware shall protect the camera and lens assembly.
- 2.8.2.4. The camera shall be high resolution colour (min. 480 TVL), and must automatically switch the camera from colour to black and white mode in extreme low light conditions. All models shall feature a 1/3" - 4-9mm vari-focal auto iris lens.
- 2.8.2.5. The outdoor camera shall offer protection against the elements and include thermostatically controlled heaters that allow operation in extreme temperatures. The camera's operating temperature range shall be -40° to 50° Celsius (-40° to 122° F).
- 2.8.2.6. The camera must perform to published specifications with either 12 or 24VAC or DC, and must automatically detect the applied voltage.
- 2.8.2.7. Cameras shall not be monitored at any off-site location.
- 2.8.2.8. Output shall be restricted for viewing only by authorized persons.
- 2.8.2.9. Dummy or unconnected cameras are not permitted.
- 2.8.2.10. Standard of Acceptance:
American Dynamics, Pelco, Panasonic
- 2.8.3. Digital Video Recording (DVR) System
 - 2.8.3.1. All cameras to be recorded with new DVR with sufficient capacity to accept all cameras with 20 % spare capacity as required at time of installation.
 - 2.8.3.2. The DVR shall include all necessary software (including an operating system) and have a time/date generator and emergency and alarm recording features.
 - 2.8.3.3. The DVR shall have the ability to record all images in a proprietary file format.
 - 2.8.3.4. The DVR must have the ability to output to a DVD/R or CD/R and shall be complete with all programs and equipment required to view images on PC screen, including a keyboard, monitor and mouse.
 - 2.8.3.5. DVR to be located in a secure location of the WSI choosing.
 - 2.8.3.6. DVR to be fully programmed to provide suitable recording times (as per client requirements).
 - 2.8.3.7. Standard of Acceptance:
Intellex, Pelco, March Networks
- 2.8.4. Monitors
 - 2.8.4.1. Monitors to be located as per WSI requirements.
 - 2.8.4.2. All monitors shall be high resolution, flat screen LCD type – minimum 17".
 - 2.8.4.3. Standard of Acceptance:
American Dynamics, Pelco, Panasonic

2.9. PERIMETER ALARM SYSTEMS

2.9.1. General

- 2.9.1.1. Experience with outside alarm systems has shown that they have a very high incidence of false alarms; these can be caused by one or more of the following:
 - .1 Movement of animals activating electromagnetic, seismic or light beam alarm systems;
 - .2 Animals moving against a fence or similar vibration system;
 - .3 Wind carried paper, plastic bags or other debris activating alarms;
 - .4 High winds causing fences to vibrate and set off alarms;
 - .5 Accumulations of surface water or snow activating electromagnetic and similar systems.
- 2.9.1.2. Exterior alarm systems are most suited to locations where a full-time overnight security patrol can immediately investigate an activated alarm signal to determine its cause (either directly or with the aid of CCTV cameras).
- 2.9.1.3. If a full-time overnight security patrol is not used, a full perimeter fence should be erected to keep animals out and reduce the incidence of blowing debris.
- 2.9.1.4. Equipment for outside alarm systems may consist of one or more of the following:
 - .1 Perimeter beam systems
 - .2 Fence vibration systems
 - .3 Ground vibration (seismic) systems
 - .4 Electromagnetic field systems
 - .5 Closed circuit television systems

2.9.2. Perimeter Beam Systems

- 2.9.2.1. Each beam tower shall be set up so that the alarm and tamper loops are together and there will be a separate environmental loop.
- 2.9.2.2. Beam towers to be configured so that the beams are set up in a "crossfire" pattern.
- 2.9.2.3. All beam towers to be equipped with thermostatically controlled heaters.
- 2.9.2.4. All perimeter beam zones to be on a separate partition (i.e. - compound partition). This partition will be independent of all other alarm system partitions.
- 2.9.2.5. Each perimeter beam to be an individual alarm zone (i.e. – not ganged).
- 2.9.2.6. Designated zones may be shunted as required by operational conditions.
- 2.9.2.7. Disarming the partition compound will shunt all designated perimeter beam zones.

Security System Specifications

Accommodation and Real Estate Services (ARES)

- 2.9.2.8. Beam towers are to be mounted and bolted directly onto contractor supplied 305mm (12") diameter concrete pedestals (sunk minimum of 813mm - 32" into the ground).
- 2.9.2.9. All cabling for the beam systems to be installed in appropriately sized plastic conduit (min. 20mm - 3/4"). All conduits to be buried to a minimum of 900 mm (36").
- 2.9.2.10. All cabling to be weatherproof and shall meet the manufacturer's specifications.
- 2.9.2.11. AC power (120V) for the perimeter beam system will be a separate circuit, and the circuit # shall be identified at the perimeter beam system panel.

Standard of Acceptance:
Takex BT or Optex Rednet series

----- End of Security System Specifications -----