SHARED SERVICES BC (SSBC)

SECURITY SYSTEM SPECIFICATIONS - 2012

Table of Contents

1. GENERAL

1.1. OVERVIEW

.1 Shared Services BC (SSBC) electronic security systems will include intrusion alarm and may include, panic duress alarm, card access, intercom, CCTV and Perimeter Alarm systems, where applicable.

.2 For the purposes of these specifications SSBC shall mean SSBC or their appointed representative WSI (Workplace Solutions Incorporated).

1.2. RELATED DOCUMENTS

.1 Privacy Guidelines – Freedom of Information and Protection of Privacy Act (FOIPP)
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

.2 Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies
http://www.cio.gov.bc.ca/cio/priv_leg/foippa/guides_forms/video_security.page

.3 WSI CMMS Information Control Sheet (ICS)

.4 WSI Contractor Health, Safety & Environmental Policy Handbook

1.3. REFERENCE STANDARDS

.1 All materials, workmanship and/or installation practices and activity shall meet or exceed the following reference standards:

.1 Canadian Electrical Code (CEC) Part 1 C22.1-00. BC Amendments to the CEC & associated bulletins

.2 BC Electrical Safety Act

.3 British Columbia Building Code

.4 British Columbia Fire Code Regulation

.5 CAN/ULC-S319-05 Electronic Access Control Systems

.6 ULC S317-96 Standard for Installation of CCTV Systems for Institutional & Commercial Applications

.7 TIA/EIA 568-B.1 through B.3 Commercial Building Telecommunications Cabling Standards

.8 TIA/EIA 569- B Commercial Building Standard for Telecommunications Pathways and Spaces

.9 ANSIA/TIA/EIA - 607A (J-STD-607-A-2002) Commercial Building Grounding and Bonding

.10 Work Safe BC, Workers Compensation Act – Part 3 – Occupational Health & Safety

.11 Applicable Federal, Provincial and Municipal laws, regulations and bylaws

1.4. GENERAL CONDITIONS

.1 Contractor shall be fully trained and factory certified on all security systems as required by this document.

.2 SSBC will have complete control of the operation of the system(s) while the building is occupied by SSBC or its tenants.

.3 All equipment shall remain the sole property of SSBC and the installing company will not retain ownership or control of the system.

.4 All hardware and software (including the Windows operating system) required to make programming changes to the card access and CCTV system(s) shall be included with the system. Hard copies of all software licenses shall be provided.

.5 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).

.6 Coordinate and cooperate with other trades for timely completion of the Work.

.7 All exceptions to these standards and specifications (including the determination of equivalencies) shall be at the sole discretion of SSBC.

1.5. LICENCES, APPROVALS, PERMITS, & STANDARDS

.1 The contractor shall be responsible for all permits, licenses, inspections and related fees.

.2 Prior to execution of work, the Contractor shall obtain all necessary permits and licenses for compliance with Federal, Provincial and Municipal laws and regulations.

.3 The contractor must be provincially licensed by the Security Services Act of the Ministry of Public Safety and Solicitor General to install alarms (SSA - 2007).

.4 The installation and commissioning of all electronic security systems shall be by qualified alarm service technicians who shall be licensed by the Security Services Act of the Ministry of the Solicitor General (SSA - 2007).

.5 The contractor shall not sub-contract any portion of the installation without prior approval of SSBC.

1.6. WORK WITH OTHERS - COORDINATION

.1 All SSBC intrusion alarm accounts will be monitored by SafeLink

.2 Security installation contractor(s) shall coordinate work with SSBC and their appointed representatives to insure alarm systems are installed, programmed, tested, commissioning and verified fully operational with SafeLink Central Monitoring Station to the satisfaction of SSBC. Refer to specification Section 2.3.

1.7. DOCUMENTATION

.1 The contractor shall provide the following documentation for each system:

- .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

.11 Warranty Certificate

.2 All documentation to be submitted electronically to WSI-CMMS group at CMMS@wsi-bljc.com and to Safelink.

.3 Contractor shall provide SSBC 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.

1.8. TRAINING

.1 Training shall be provided for each individual system as required by this document. Training shall include a minimum of two (2) hours per individual system and shall be conducted at a time that is mutually agreeable to both the contractor and SSBC.

1.9. WARRANTY

.1 The warranty period with respect to the Contract is one (1) year from the certified date of Substantial Performance of Work.

.2 Defective equipment to be repaired at site, and failing this a suitable replacement unit shall be supplied to keep the system operational until the original unit is returned.

.3 Warranty certificate must include all Company contact information (address, contact person(s), telephone (regular hours and emergency after hours, fax and email) with master Maintenance Manuals.

2. SECURITY SYSTEMS

2.1. OPERATIONAL REQUIREMENTS

.1 Electronic security systems installed in Shared Services BC (SSBC) facilities shall operate on a 24-hour basis throughout the year.

.2 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 backup 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).

.3 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.

2.2. PRODUCTS - GENERAL

.1 All products being delivered shall be from reputable industry recognized manufacturers regularly engaged in the production of models and types of equipment used in the electronics security, computer, and telecommunications industries. Products shall be quality control tested and verified for the intended operation prior to installation at site.

.2 Products shall conform to the standards of the Canadian Standards Association or CSA recognized approved equivalent. All materials, including hardware and software being supplied, shall be new and of the latest version or production model.

.3 Equipment specifications are intended to provide a baseline reference for the type of materials that are to be installed. Contractor shall insure that all equipment being offered meets or exceeds the minimum requirements for intended operation.

.4 Reference manufacturer's products have been approved as standard equipment for installation at SSBC facilities and shall not be substituted or replaced with un-approved alternates without written approval from SSBC.

2.3. INTRUSION ALARM SYSTEM

.1 General

.1 The protected space shall be provided with a complete intrusion alarm system. Intrusion protection shall be provided by way of door contact switches, and motion sensors (Note: glass break detectors used only in consultation with SSBC). The intrusion alarm system is designed to detect unauthorized entry into protected spaces. The system shall conform to the requirements of this document.

.2 The intrusion alarm system may be divided into separate partitions (areas).

.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).

.4 Home-run all devices to the alarm panel - do not gang or group devices unless otherwise authorized in writing by SSBC.

.5 The system shall have the capacity to provide one access code per person for the full occupancy of the protected space. Each user or user group to have an individual user code.

.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

.7 Security panel make and model shall be approved in advance by SSBC. The panel shall be non-proprietary (i.e. – available to all alarm contractors).

.8 The panel power transformer 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 electrical circuit # be clearly identified on both the electrical panel directory and on the alarm panel.

.9 Battery backup shall be gel-cell type, minimum 7 amp/hour. Battery installation date shall be marked on the battery and panel cover.

.10 All devices (including the panel) shall be supervised with tamper switches and end of line resistors.

.11 EOL devices shall be installed at the device – not in the panel.

.12 A copy of the zone descriptors shall be left inside the alarm panel.

.13 Installation includes field equipment, mounting hardware, wiring, terminations and I/O modules required to support the various alarm points and/or alarm systems, programming and setup of all field devices.

.14 Telecommunication closets shall be protected by the intrusion alarm system and shall be included in the overall main office intrusion alarm system. Each telecommunication room to have the following equipment:

.1 All doors equipped with door contacts.

.2 Allow for one motion detector to be installed in each telecommunications closet.

.15 All environmental alarms to be 24-hour zones, activated for continuous monitoring.

.16 Provide siren in the protected space, to alert staff of an alarm condition

.17 Standard of Acceptance:
DSC 4020, 1832 and 1864 series (most current versions)

.2 **Programming**

.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 SSBC monitoring station.

.2 SSBC shall supply the contractor with all access codes and phone numbers to be programmed into the alarm system.

.3 The panel shall be programmed in SIA or CID format.

.4 The contractor shall program the following:

.1 User code required to bypass zones

.2 Daily test transmission (after 00:01 – 5:00, but 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

.7 Remote download access enabled

.8 Access &panel upload codes left at default

.9 Installer code left at default

.5 The contractor shall not install a contractor's lockout enable and shall not program Forced Arming or Auto-Disarming without prior approval from SSBC.

.6 Upon completion of programming the installer shall initiate an upload of the panel programming to Safelink (SSBC authorized monitoring agent).

.7 Once the system installation is completed, the contractor shall not access the system either physically or electronically without SSBC approval.

.3 **Monitoring**

.1 SSBC retains the right to monitor their alarm systems in the manner of their choice and will not be locked into any other monitoring arrangements as a result of alarm system installations.

.2 Contractor shall provide connectivity (hardware & software) with Safelink monitoring station as directed by SSBC. Methods include, but are not limited to:

.1 Network connection, with telephone backup;

.2 Network connection, with cellemetry (in the event that both network and phone line fail) and telephone communicator setup as the 3rd level of backup;

.3 Telephone connection with cellemetry backup.

.3 All options must be set up with single primary reporting path. Backup communicators will operate as secondary path if the primary communication path fails to operate successfully

.4 Monitoring is arranged by WSI, Refer to Section 3.5.

.5 In the event that the client's fax line is to be used as the primary communications line, the demarcation point must be marked "Do Not disconnect without informing WSI". Do not use VOIP communication for any security monitoring applications.

.6 All telephone jacks used for alarm/security systems shall be wired to USOC RJ31 industry standards. All position eight (8) jacks shall be installed with a tamper loop, ahead of the demark block.

.7 WSI shall issue all phone numbers for monitoring and downloading. All intrusion alarm systems shall be connected to analogue telephone lines - no VOIP (voice over internet) lines.

.4 **Keypads**

.1 No global keypads - each partition will have its own keypad

.2 All keypads shall be LCD alpha (full English) type (unless otherwise specified)

.3 All keypad panic buttons shall be disabled

.4 All keypads to be set up for "Quick Arming" ("*–0")

.5 All keypads to be installed at 1.372m (54") above finished floor.

.5 **Network Alarm Communicator**

.1 Where required, contractor shall provide network alarm communicator interconnected to intrusion alarm system for reporting alarms over client LAN/WAN Ethernet infrastructure.

.2 Network alarm communicator shall connect to the Building Utility Subnet (BUS). The BUS enclosure to be a separate zone on the overall intrusion alarm system. For details on the BUS enclosure see Technical Standards Section 12 – Technical Standards- Structured Cabling (*w/hyperlink*)

.3 Communicator specifications:

.1 128-bit AES encryption (NIST approved)

.2 Supports DHCP (dynamic IP addresses)

.3 Low network bandwidth

.4 Compatible with 10/100BaseT networks

.5 Reports events to 2 different receiver IP addresses

.6 Polling and hardware substitution protection

.7 4 on-board programmable inputs and 2 programmable voltage outputs as stand-alone module

.8 Programmable through the T-Link Console software

.4 Standard of Acceptance: DSC TL-250

.6 **Sirens/Strobes**

.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 watts)

.2 All sirens and strobes to be on an isolated power supply.

.3 All systems shall be programmed for 4 minute bell duration.

.4 An exterior strobe (blue) shall be installed for all systems, location to be decided in consultation with SSBC (strobe may be mounted inside a window within the protected space - provided the strobe is visible from the exterior of the building).

.5 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.)

.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. Additional sirens or tone devices to be located throughout the protected space so that all staff can hear the alert.

.7 Standard of Acceptance:
Interior Sirens – Honeywell WAVE-2F, Ademco 747
Exterior strobe/siren (blue) - Amseco SSX 52SB, ATW PR-DOBERMAN

.7 **Motion Detectors**

.1 Motion detectors shall only be dual technology type (PIR and microwave).

.2 All motion detectors shall be field-adjusted as per manufacturer's specifications for full coverage pattern of the protected spaces. Dual tech 360° detectors may be installed where applicable.

.3 All motion detectors shall have LED's disabled after initial testing is done.

.4 Standard of Acceptance:

Optex MX Series, DSC LC-104, Honeywell DT series;
360° Motion Detector: Bosch DS9360

.8 **Glass Break Devices**

.1 All devices shall be installed and field-adjusted as per manufacturer's specs.

.2 Standard of Acceptance:
GE SR-5815NT, Honeywell FG1625

.9 **Door/Window Contacts**

.1 Every door which leads to the protected space shall be fitted with a door contact switch.

.2 All grade level or easily accessible opening windows shall be equipped with a contact.

.3 All door contacts shall be installed at the top of the door, opposite the hinge side of the door.

.4 All door and window contacts must be "wide gap" type.

.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.

.6 Standard of Acceptance:
GE Sen1078 series, Amseco AMS-25A/B,
Overhead doors: GE SEN2200, GE2315A-L, Amseco ODC-59A/B

.10 **Cellemetry Back-Up**

.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 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.

.3 Digital Cellemetry panel must be installed in a location that is physically and visually separated from the main alarm panel (so that intruders cannot readily find the cellemetry panel to disable it).

.4 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.

.5 Standard of Acceptance:

DSC GSM Alarm Communicator Model GS3060 http://www.dsc.com

Uplinks model 2550 http://www.uplink.com

2.4. PANIC ALARMS

.1 **General**

.1 Panic alarms shall be activated by a hardwired panic button(s).

.2 Panic buttons to be strategically located, suitably sized and identified/clearly labeled for “security emergency”.

.3 All panic buttons shall be clearly identified by a label (Brother P2000 or equivalent).

.4 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 **Local Response Systems (Not monitored)**

.1 Unless specified, the panic alarm system shall be a separate, standalone system and will not be monitored.

.2 Local panic systems will not be integrated into the main intrusion alarm panel.

.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).

.4 Where multiple panic alarm locations are provided, a standalone panel shall be installed.

.5 Each standalone panic alarm panel will be controlled by an LED keypad that will clearly identify the location of each panic button.

.6 If more than 16 panic buttons are required then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panels

.7 Make and model of panic button shall be decided in consultation with SSBC.

.8 Standard of Acceptance:
Multi-zone non-monitored panel: DSC 1832 or 4020

Annunciator panels (16 + zones or more): DSC 4632 and DSC 4664
Panic button: Potter HUB-M (non-latching), HUB-DL-L (Latching LED), GE Sentrol 3045 (non-latching LED)

.3 **Monitored Panic Alarm Systems**

.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 panel(s).

.2 SSBC and/or the client 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).

.4 **Wireless Panic Alarm Systems**

.1 Wireless panic alarms shall only be installed at the direction of SSBC.

.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

.3 Standard of Acceptance:
Visonic MCT 201, MCT 124; Honeywell 5802 MN2, Innovonics EchoStream

2.5. REMOTE DOOR CONTROL

.1 Designated door(s) will have a selector switch that will enable the door to be remotely locked or unlocked during business hours.

.2 The selector switch shall be interfaced with the card access system.

.3 The selector switch will be clearly labeled “Open” and “Locked”.

.4 Standard of Acceptance:
Camden CM 190/4

2.6. REMOTE DOOR RELEASE

.1 Designated door(s) will have a push button that will enable the door to be remotely released during business hours.

.2 The push button is to be interfaced with the card access system.

.3 The push button will be clearly labeled as to which door is controlled.

.4 Standard of Acceptance:
Camden CM 9280

2.7. ACCESS CONTROL SYSTEMS

.1 **General**

.1 Access control system shall be installed in protected space based on client requirements. 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 The system shall be capable of expanding to allow for a minimum of 20% additional card readers.

.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%.

.4 The access system will be interfaced with the intrusion alarm system so that access cards can disarm the intrusion alarm system, unless otherwise noted. The access system shall disarm by first user in (not auto-disarm).

.5 The card system shall be programmable and shall allow users to determine which doors can be accessed and at what time of day

.6 Every door equipped with a card reader and electric locking device shall also have a door contact to monitor held open/door forced open functions and request to exit (REX) motion sensor.

.7 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.

.8 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.

.9 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.

.10 All readers to be installed at 1.2m (46") above finished floor unless directed otherwise by SSBC.

.11 Standard of Acceptance:
Kantech Entra-Pass Special (most current version).

Kantech Main Controller to be KT400; sub-controllers to be KT300 (no KT200).

26 bit HID cards/fobs (client choice).

.2 **Card Readers**

.1 Reader shall be connected to door controller via standard Wiegand interface.

.2 Bi-color LED controlled locally and by host system shall provide at the minimum following visual feedback: (RED = door locked, GREEN = access granted).

.3 Built in beeper controlled locally and by host system shall provide distinctive acoustic feedback when: card is read, access is denied, during door-ajar pre-alarm and during door alarm.

.4 Exterior card reader shall be weather proof, designed for outdoor applications and installed on gasketed watertight boxes with drain hole at the bottom.

.5 All wall-mounted readers shall be designed for installation on a standard single-gang electrical back-box.

.6 Mullion sized readers may be used only in locations with limited mounting space.

.7 Standard of Acceptance:

HID 5395 ThinLine II wall mount; HID 5365 Mini-Prox mullion type.

.3 **Request to Exit Detector (REX)**

.1 Request to Exit (REX) motion sensor will allow egress through monitored doors without creating alarms with REX connected to bypass door alarm on exit. REX must be configured to shunt door alarm, not unlock it.

.2 The motion detector shall have a build-in buzzer to locally annunciate “door forced” alarms and “door held open” warnings.

.3 REX sensors shall have the following minimum features:

.1 X-Y Targeting - targets a specific area of detection

.2 Digital Signal Processing

.3 Curtain type Fresnel lens

.4 Detection range 3 to 6 meters

.5 Main relay timer (adjustable delay .5 to 60 seconds)

.6 Selectable relay trigger mode

.7 Sounder volume to 90dB

.8 Activation LED

.9 Tamper switch

.4 Standard of Acceptance:
Kantech T-Rex

.4 **Electric Strikes**

.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 Unless otherwise directed electric strikes shall fail “secure.”

.3 All electric strikes shall be 12/24 volt dc.

.4 Standard of Acceptance:
Rutherford, Securitron, Folger Adam, HES

2.8. AUDIO INTERCOM

.1 The audio intercom unit will be installed adjacent to the designated entry door at 1.4 m (54") AFF. Master station will be desk or wall mounted in a location of the client's choosing, typically at reception or administration offices.

.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.

.3 Standard of Acceptance:
System - Aiphone IE Series Master station, Exterior door station - IE-SS

2.9. VIDEO INTERCOM

.1 The video intercom unit will be installed adjacent to the designated entry door at 1.4 m (54") AFF. Master station will be desk or wall mounted in a location of the client's choosing, typically at reception or administration offices.

.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.

.3 Standard of Acceptance:
Aiphone MK-1GD (B+W), KC Series (colour), Exterior door station – MK-DVF (B+W), KB-DVF (colour)

2.10. CLOSED CIRCUIT TELEVISION (CCTV) SYSTEMS

.1 **General**

.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.cio.gov.bc.ca/cio/priv_leg/foippa/guides_forms/video_security.page

.2 CCTV system to be on separate, standalone network and will not be connected to the government network. Cameras shall not be monitored at any off-site location.

.3 The CCTV system shall include all equipment necessary for a fully functioning system.

.4 Closed circuit television systems shall be designed and installed by certified personnel.

.5 Cameras installed in high sensitivity areas will provide full visibility of person(s) entering the area. Cameras must be mounted at suitable height for the required field of view, for clear unobstructed viewing.

.6 Cameras shall be monitored either by an operator and recorded locally. Output must be available for viewing by authorized persons. Cameras shall not be monitored at any off-site location.

.7 Indoor/outdoor camera enclosures must be vandal resistant domes constructed of high impact polycarbonate material.

.8 Outdoor cameras will include thermostatically controlled heaters that allow operation in extreme temperatures.

.9 CCTV workstation(s) will include an LCD monitor installed at designated operator locations.

.10 Video signal cabling for interconnection between equipment shall be minimum RG-59 type, solid bare copper center conductor with minimum 95% copper braid shield.

.11 Where IP network cameras are installed, wiring shall be UTP CAT5e data cable in compliance with EIA/TIA 568 Standards.

.12 Cables placed in underground ducts and outside of buildings shall be rated for outdoor use with water blocking members.

.13 CCTV systems shall be protected from lightning and power surges.

.2 **Cameras**

.1 All cameras shall be powered from a CSA (or equivalent rated) approved camera manufacturer power supply. All connections shall be crimped.

.2 Unless specified otherwise, all cameras shall be dome type. Indoor/outdoor camera enclosures with vandal resistant domes constructed of high impact polycarbonate material, plenum rated back box and UV resistant smoked optically clear acrylic lower dome with maximum of f/0.5 light loss and tamper resistant hardware. Diameter of lower dome will be low profile, maximum 6”

.3 The camera shall be high resolution colour (min. 480 TVL, 640 x 480), 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” vari-focal auto iris lens, suitable to provide coverage of the area being viewed.

.4 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).

.5 The camera shall operate on 12 or 24VAC or DC, and must automatically detect the applied voltage.

.6 Dummy cameras are not permitted.

.7 Where IP cameras are installed, all cameras and converters shall be H.264 compliant, with capability to fully integrate with Genetec systems. Contractor shall consult with SSBC prior to installation to confirm that products being installed are acceptable.

.8 All exterior cameras shall utilize surge protectors to protect against lighting strikes.

.9 Standard of Acceptance:
American Dynamics, Pelco, Panasonic, Sony, Avigilon

.3 **Digital Video Recording (DVR) System**

.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 The DVR shall include all necessary software (including an operating system) and have a time/date generator and emergency and alarm recording features.

.3 The DVR shall have the ability to record all images in a proprietary file format.

.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.

.5 DVR to be mounted in a secure location as directed by SSBC. Contractor shall coordinate final mounting location at site prior to installation.

.6 DVR to be fully programmed to provide suitable recording times (as per client requirements).

.7 Standard of Acceptance: American Dynamics – Intellex

.4 **Monitors**

.1 Monitors shall be wall or desk mounted as per SSBC requirements.

.2 All monitors shall be high resolution, TFT active matrix LCD monitor, with multimode functionality, minimum 1280 x 1024 resolution – minimum 21".

.3 Standard of Acceptance:
American Dynamics, Pelco, Panasonic

2.11. PERIMETER ALARM SYSTEMS

.1 **General**

.1 Equipment for exterior alarm detection 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 **Perimeter Beam Systems**

.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 Beam towers to be configured so that the beams are set up in a "crossfire" pattern.

.3 All beam towers to be equipped with thermostatically controlled heaters.

.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.

.5 Each perimeter beam to be an individual alarm zone (i.e. – not ganged).

.6 Designated zones may be shunted as required by operational conditions.

.7 Disarming the partition compound will shunt all designated perimeter beam zones.

.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).

.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")

.10 All cabling to be weatherproof and shall meet the manufacturer's specifications.

.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.

.12 Standard of Acceptance:
Pulnix, Takex BT or Optex Rednet series

2.12. SYSTEM CONDUCTORS & CABLES

.1 Provide wiring as required for all components. Unless specified otherwise, selection of cable type shall be as per manufacturer's recommendations.

.2 All copper and fiber cable sheaths shall meet fire code requirements and comply with all applicable codes and meet all standards as required by the local AHJ (Authorities Having Jurisdiction).

.3 Contractor shall be responsible for insuring that all conductor types and gauges required to adequately power and control all equipment being installed for use with their system.

.4 All wiring shall be concealed unless otherwise authorized by SSBC.

.5 Video signal cabling for interconnection between equipment shall be minimum RG-59 type, solid bare copper center conductor with minimum 95% copper braid shield. For cable runs over 100 meters in length, RG-6 cable may be used. All CCTV coaxial cable connections shall be made using crimped or pre-manufactured connectors only.

.6 Where IP network cameras are installed, wiring shall be UTP CAT5e data cable terminated on CAT5e modular jacks connected to digital video equipment (or managed PoE network switches). CAT5e cabling shall be supplied, installed,

terminated and tested to fully meet EIA/TIA 568 Transmission Performance Specifications.

.7 Cables placed in underground ducts and outside of buildings shall be rated for outdoor use with water blocking members.

.8 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 (Marrette connectors are not allowed).

.9 Security RS-485 communication cabling shall be routed away from voice/data cables to prevent interference.

3. EXECUTION

3.1. INSTALLATION

.1 Installation shall be in accordance with the manufacturer's specifications and installation procedures and fully comply with all applicable Codes & Regulations.

.2 Contractor shall test and commission fully operational and functional systems prior to turnover to the SSBC. SSBC reserves the right to verify the contractor’s test results to determine if system operation is satisfactory and contractor will be responsible to correct any deficiencies at no additional cost to SSBC

.3 All cables shall be permanently identified and listed on as-built drawings as follows:

- .1 Cable number
- .2 Source
- .3 Destination

.4 Electrical panel circuit number shall be clearly identified on all system panels.

.5 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.

.6 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.

.7 Contractor shall repair at no cost to the Owner, any surfaces, finishes, equipment or structures damaged by the execution of their contract to its original condition.

3.2. SECURITY TERMINATION

.1 All security system 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). Head-end security equipment for Access Control and CCTV shall be mounted at locations designated by SBBC.

3.3. GROUNDING AND BONDING FOR ELECTRONIC SECURITY

.1 Ground security equipment as per manufacturer's recommendations.

.2 Bonding conductor shall be green PVC jacketed, stranded copper, soft conductor, unless otherwise noted.

.3 Follow J-STD-607-A-2002 (CSA-527) Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications and the most current version of the CEC.

3.4. PATHWAYS FOR ELECTRONIC SECURITY

.1 Unless otherwise specified, SSBC security systems do not require conduit – except in exposed or exterior locations however all wiring shall be concealed unless otherwise authorized by SSBC.

.2 All wiring and cable installed and connected to any piece of security equipment that is accessible to the public shall be installed in conduit or protective covering. Conduit connecting to field devices such as camera enclosure shall be terminated and secured up to the enclosure to conceal all wiring and connections. Where applicable, the security contractor shall coordinate installation of conduit and raceways with electrical contractor to meet these requirements. Conduit not to be filled past 40% capacity.

3.5. PROCEDURE FOR ACTIVATING & COMMISSIONING ALARM MONITORING

.1 General Overview

.1 All alarm systems and ancillary equipment shall conform to the SSBC Security System Specifications.

.2 Account numbers and all IP information shall be provided by Safelink monitoring station.

.3 The security installation contractor must download the following forms from Safelink:

.1 Alarm System Installation Report

.2 Zone List

.3 User List

.4 Installation Checklist

Safelink contact information:

Phone #: 604-454-1085 , email address: data@paladinsecurity.com

.2 Contractor Responsibilities

.1 The contractor shall insure that all required information is provided and recorded on the Safelink forms (as per 3.5.1.3) to facilitate programming and activation of the account with Safelink.

.2 The contractor shall complete the User list in conjunction with the client (tenant) who will provide details of appropriate users. Contractor shall fully program the system with this information.

.3 Contractor shall compile information required on forms and submit the completed electronic documents to both WSI (CMMS@wsi-bljc.com) and Safelink (data@paladinsecurity.com).

.3 Client (Tenant) Responsibilities

.1 Once the system is installed and commissioned the client (tenant) is responsible to manage the Client User List function and maintain the database ensuring that all subsequent changes to personnel are noted and reported to WSI (Safelink).

.2 All Information is “Confidential” and will provide a record of authorized users to the monitoring company and therefore is to be kept in a secure location on site.

4. APPENDIX

4.1. SAFELINK ALARM INSTALLATION REPORT

4.2. INTRUSION ALARM

.1 IAS-SKE-01 Typical Interconnection

4.3. ACCESS CONTROL TYPICAL LAYOUT

.1 ACS-SKE01 - Typical Interconnection

.2 SK-01 – Single Door Card reader w/RTE PIR exit

.3 SK-01 – Exterior Alarmed door w/ RTE PIR alarm shunt/sounder

4.4. CCTV TYPICAL LAYOUT

.1 CCTV- SKE01 – Typical Interconnection

.2 SK-02 Dome camera “drop” ceiling mount

.3 SK-02 Exterior Environmental dome camera pole mount

.4 SK-03 Dome camera surface mount

.5 SK-03 Dome camera recessed wall mount

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

Print Form

Alarm System Installation Report

Building Information (to be completed by WSI):

Building Number		Date of Request	
Street Address		City	
Tenant (site name)		Premise ph number	
Tenant contact name		Tenant contact phone	
Tenant contact email			

○ Existing system ○ Retrofit or upgrade ○ New Installation ☐ Work being performed PRIOR to tenant occupancy

Briefly describe scope of work			
Name of contractor who will perform work:		Contact phone	
Contractor email			
BCB #			

Monitoring Information will be provided by Safelink upon receipt or work order with BCB#:
Safelink contact info: phone 1-604-454-1085, or email data@paladinsecurity.com

Internet account #	
GSM account #	
Account number	

Communication details such as receiver phone numbers, IP addresses, and account numbers will only be issued upon receipt of a work order issued by WSI which authorizes the installing company to perform the stated work.

All system installation and service work shall be done in accordance with the SSBC Installation Standards.
http://accommodationandrealestate.gov.bc.ca/Doing_Business_With_Us/Technical_Manuals

Contractor Form

Contractor Information:

Contractor name | Phone Number

Address | Fax Number

City | Prov. | Postal Code | BC Elec. Contractor #

BC Security License # | website

Lead Technician | TQ # | Tech Phone #

System Information:

Alarm panel make/model | Reporting format | # Partitions

Elec Permit # | Alarm Permit # | Panel demark phone number

Panel location (describe)

Communications Information:

Primary communication ☐ Dialer ☐ GSM cell back-up ☐ Internet (on BUS system)

Secondary communication ☐ Dialer ☐ GSM cell back-up ☐ Internet (on BUS system)

If GSM, what type? ☐ DSC GS3060i ☐ GE AnyNet (will depend on available cellular coverage in area)

If internet enabled, IP address of comm device | Gateway | Subnet Mask

Contractor installation checklist:

- ☐ Zone descriptions entered, partition labels programmed
- ☐ Daily test programmed between 12:01 am and 5:00 am
- ☐ Open /close reporting programmed by user, not by partition
- ☐ Group or partition open/close NOT programmed
- ☐ All keypad panics disabled
- ☐ Siren time-out set to 4 minutes
- ☐ Answering machine override enabled
- ☐ Remote download access enabled; access and panel upload codes left at default
- ☐ Installer code left at default (lockout NOT enabled)
- ☐ User code required to bypass zones
- ☐ All PIR zones have LEDs disabled
- ☐ All PIR zones walk-tested for appropriate coverage
- ☐ Panel programmed to report to Safelink monitoring station
- ☐ All zones tested to Safelink monitoring station
- ☐ Manuals left on-site with user representative
- ☐ Users / user representative trained on system use
- ☐ Zones and User Lists (attached) faxed to Safelink
- ☐ System programmed to auto-arm daily (7 days/week) at 11:00 pm
- ☐ Exterior strobe light installed (or strobe inside window visible from outside)
- ☐ Hardwired transformer(s) used (NOT plug-in) for all power requirements
- ☐ All documentation provided in electronic form, email to CMMS@wsi-bljc.com

Verification number provided by Safelink:

Verification number is required to confirm that all zones have been tested to station.

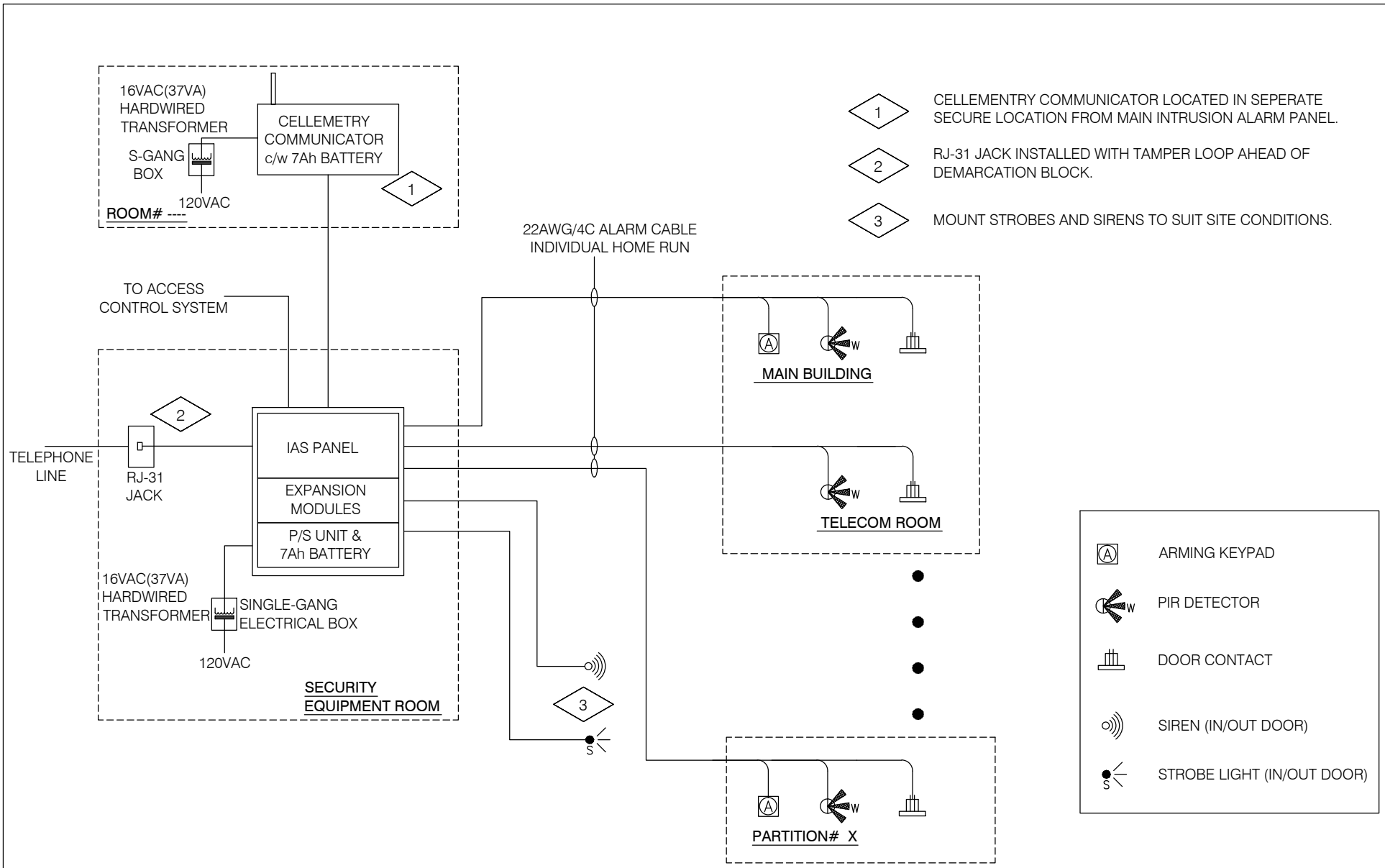
I hereby certify that this system has been installed to the Shared Services BC (SSBC) standards, and all work is complete:

Name | Date | Signature

#	Partition	Zone Description	#	Partiton	Zone Description

User List

User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	
User #		Name		Code		Pasword	

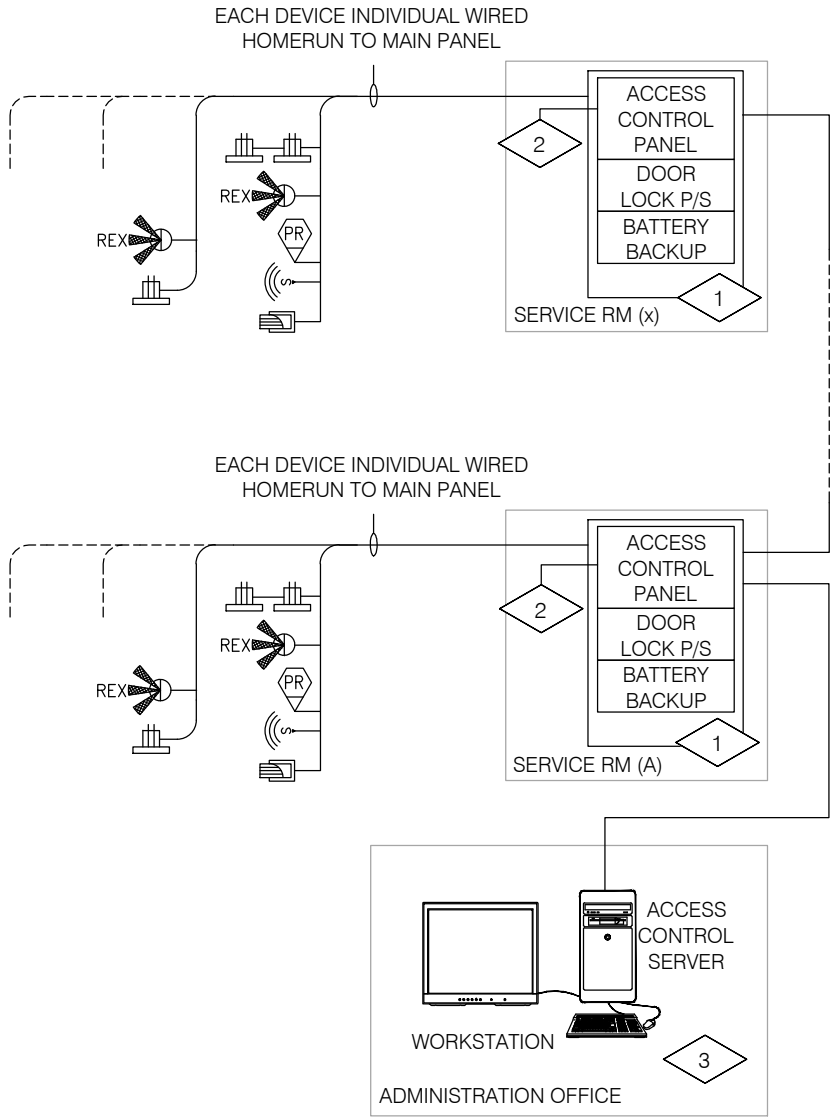


BRITISH COLUMBIA | Shared Services BC

dwg title

INTRUSION ALARM RISER
TYPICAL INTERCONNECTION

date: JULY, 2011	scale: N.T.S.
drawn by: -	project no. -
checked by: -	dwg no. IAS-SKE01



1 MINIMUM 7Ah BATTERY BACKUP. CONNECT TO UPS/EMERGENCY 120VAC POWER CIRCUIT (WHERE REQUIRED).

2 INTERFACE TO INTRUSION ALARM SYSTEM.

3 CONNECT TO UPS/EMERGENCY 120VAC POWER CIRCUIT(WHERE REQUIRED).

DOOR CONTACT

REX-PIR

PROX. READER

SOUNDER

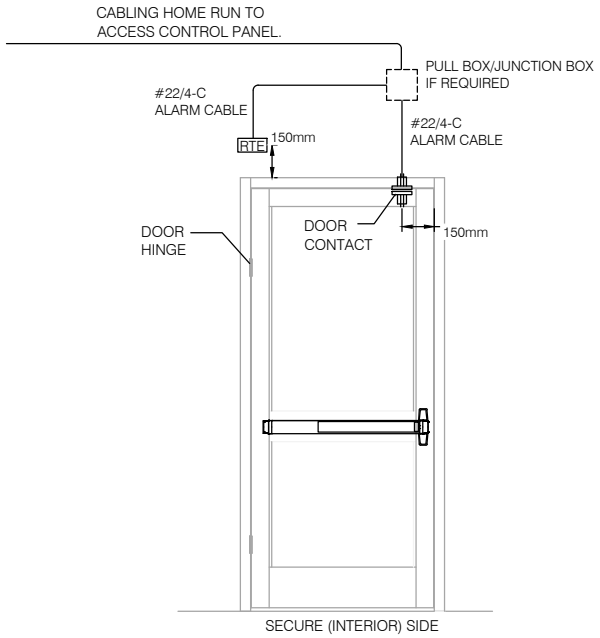
ELECTRIC STRIKE

BRITISH COLUMBIA | Shared Services BC

dwg title

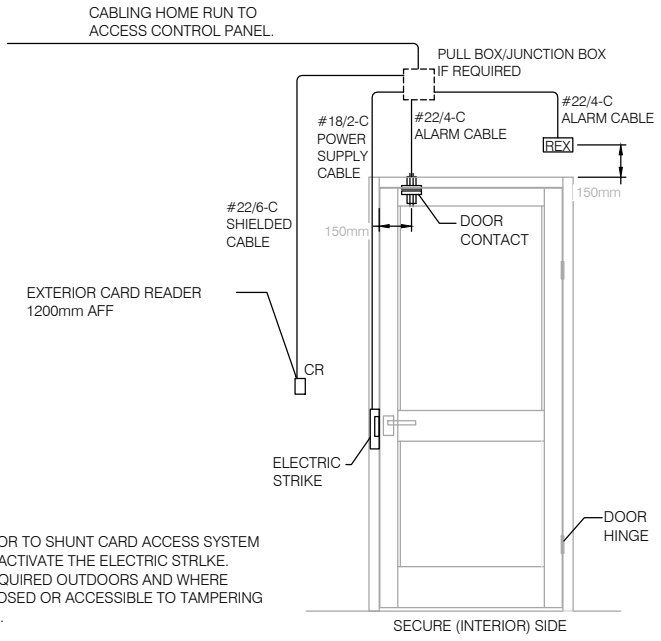
ACCESS CONTROL SYSTEM RISER
TYPICAL INTERCONNECTION

date: JULY, 2011	scale: N.T.S.
drawn by: -	project no. -
checked by: -	dwg no. ACS-SKE01



Exterior Alarmed Door

N.T.S.

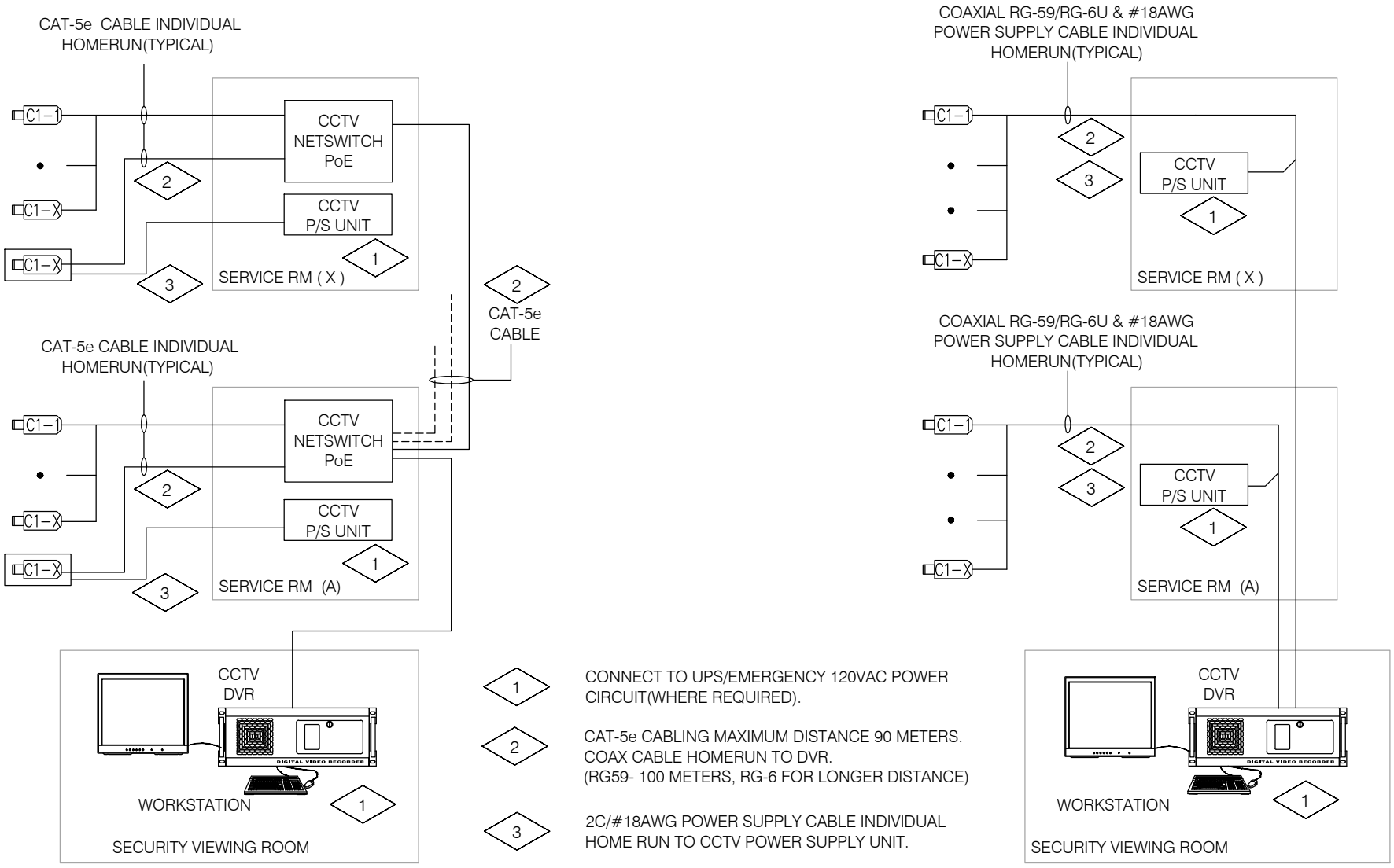


NOTE:-
- REX DETECTOR TO SHUNT CARD ACCESS SYSTEM ONLY, NOT ACTIVATE THE ELECTRIC STRLKE.
- CONDUIT REQUIRED OUTDOORS AND WHERE WIRING EXPOSED OR ACCESSIBLE TO TAMPERING OR DAMAGE.

Card Reader Door With 'RTE' PIR

N.T.S.

BRITISH COLUMBIA Shared Services BC	date: JULY, 2011	scale: N.T.S.
dwg title: TYPICAL SECURITY DOOR LAYOUTS	drawn by: -	project no. -
	checked by: -	dwg no. SSBC-SK-01



CCTV - IP NETWORK

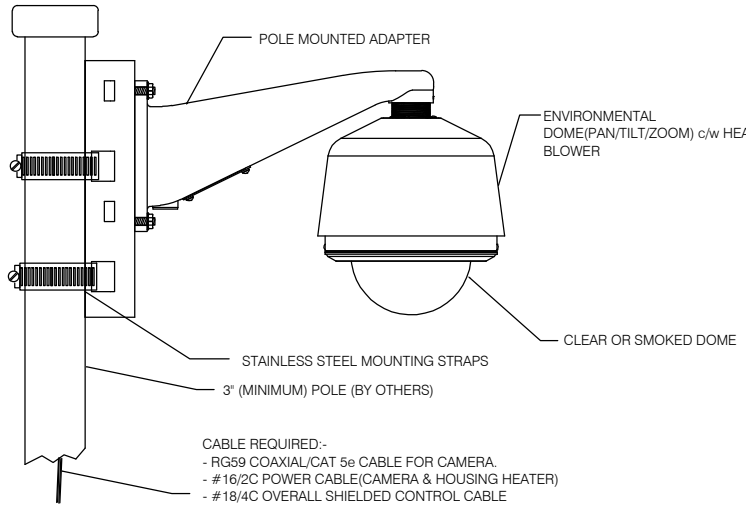
CCTV - ANALOG

BRITISH COLUMBIA | Shared Services BC

dwg title

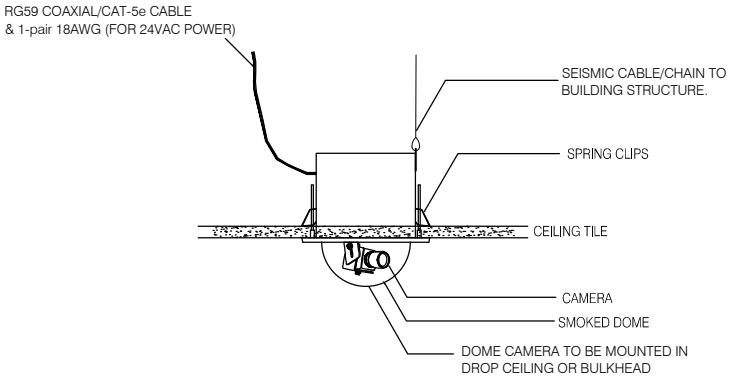
CCTV SYSTEM RISER
TYPICAL INTERCONNECTION

date: JULY, 2011	scale: N.T.S.
drawn by: -	project no. -
checked by: -	dwg no. CCTV-SKE01



Pole Mounted Environmental Dome

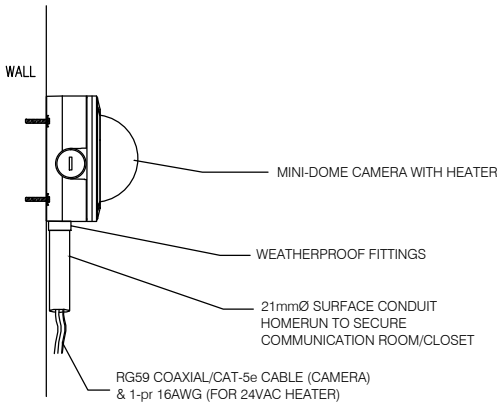
N.T.S



CCTV Dome Camera Drop Ceiling Mounted

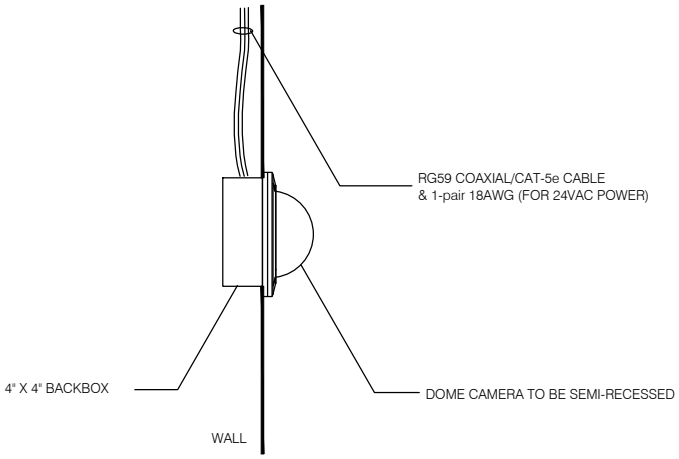
N.T.S.

BRITISH COLUMBIA Shared Services BC	date: JULY, 2011	scale: N.T.S.
dwg title	drawn by: -	project no. -
TYPICAL SECURITY CCTV CAMERA MOUNTED	checked by: -	dwg no. SSBC-SK-02



CCTV Dome Camera Surface Mounted

N.T.S



CCTV Dome Camera Recessed Wall Mounted

N.T.S.

BRITISH COLUMBIA | Shared Services BC

dwg title

TYPICAL SECURITY CCTV CAMERA MOUNTED

date: JULY, 2011	scale: N.T.S.
drawn by: -	project no. -
checked by: -	dwg no. SSBC-SK-03