SECURITY SYSTEMS STANDARDS

Date of Update	Sections Updated
06-22-2017	Sections 1-11 (Full Revision) CITZ BTA's Chris Lien / Clayton Evoy

Disclaimer

This document was prepared for the purposes of the Province of British Columbia and is not intended to be used for other purposes. This document may be revised periodically without notice and may not accurately reflect the current state of the law in British Columbia. A reference to a product or service contained in this document does not constitute an endorsement or recommendation of that product or service by the Government of British Columbia.

This document and all of the information it contains are provided "as is" without warranty of any kind, whether express or implied. All implied warranties, including, without limitation, implied warranties of merchantability, fitness for particular purpose, accuracy, completeness and non-infringement, are hereby expressly disclaimed. The information in this document may not be suitable for your purposes; any person relying upon any information in this document does so at his or her own risk.

Under no circumstances will the Government of British Columbia be liable to any person or business entity for any direct, indirect, special, incidental, consequential, or other damages based on any use of this document, including, without limitation, any lost profits, business interruption, or loss of programs or information, even if the Government of British Columbia has been specifically advised of the possibility of such damages.

1. General

1.1. Licenses, Approvals, Permits and Standards

.13 The Contractor shall be responsible for all permits, licenses, inspections, and related fees.

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

.15 The Contractor must be provincially licensed by the Registrar of Security Services as per the British Columbia Security Services Act (SBC 2007).

.16 The consulting, design/engineering, sales, installation, and commissioning of all electronic security systems shall be by qualified personnel, who shall hold all required license categories as per the British Columbia Security Services Act (SBC 2007).

.17 The contractor shall not sub-contract any portion of the installation without prior approval of the Ministry of Citizen' Services (CITZ).

1.2. Reference Standards

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

a) Canadian Electrical Code (CEC) C22.1-15; including BC specific amendments.

b) TIA/EIA-568 Commercial Building Telecommunications Cabling

c) TIA/EIA-569 Commercial Building Telecommunications Pathways and Spaces.

d) TIA/EIA-607 Telecom Bonding and Grounding

e) CITZ Technical Standards for Offices – Structured Cabling

f) CAN/ULC-S302-14 Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems.

g) CAN/ULC-S316-14 Standard for Performance of Video Surveillance Systems.

h) CAN/ULC-S318-96 Standard for Power Supplies for Burglar Alarm Systems.

i) CAN/ULC-S319-05 Electronic Access Control Systems.

j) NFPA72 Requirements for notification devices

k) British Columbia Electrical Safety Act.

l) British Columbia Building Code and Local Building Bylaws.

m) British Columbia Fire Code

n) Work Safe BC, Workers Compensation Act (Part 3) – Occupational Health & Safety.

o) All other applicable Federal, Provincial and Municipal laws, regulations, and bylaws.

1.3. 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://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/real-estate-space/video_surveillance_policy.pdf

.3 CITZ Technical Standards for Offices – Tenant Improvements
http://www.accommodationandrealestate.gov.bc.ca/Doing_Business_With_Us/Technical_Manuals/files/CITZ_Technical_Standards_for_Offices.pdf

1.4. General Conditions

.1 CITZ Security Standards shall not be altered in any way, and must be included as a complete document.

.2 These standards apply to all security related/involved devices, physical or virtual, connected to the CITZ security systems and networks.

.3 Compliance with these standards does not imply a completely secure system. Instead, these requirements should be integrated into a comprehensive site security plan.

.4 Contractor(s) shall maintain current, all licenses required to provide the specific work efforts of the project. The Contractor should utilize installation and service technicians whom are competent, factory trained and industry certified personnel capable of installing and maintaining the system, and providing reasonable service.

.5 Contractor shall take necessary measures to maintain security and prevent unauthorized access.

.6 CITZ will have complete control of the operation of the system(s), while the building is occupied by CITZ and/or its tenants.

.7 All equipment shall remain the sole property of CITZ and the installing company will not retain any ownership and/or control on, or of, the system(s).

.8 All hardware, software, and operating systems required for operation, including programming, shall be provided. Hard copies of all required licenses/keys shall be provided.

.9 All systems shall be configured to be managed (locally) onsite. Certain systems may require the ability to be remotely controlled and configured (as specifically identified on a site-by-site basis).

.10 Coordinate and cooperate with other trades for timely completion of the work.

.11 All exceptions to these standards (including the determination of equivalencies) shall be made in consultation with one of the Ministry of Citizen' Services (CITZ) Building Technology Advisors (BTA) for Security.

1.5. Material Substitutions

.1 Whenever materials, equipment or processes, are specified or described in this standard by using the proprietary name of an item, or the name of a particular manufacturer, the naming of the items is intended to establish the type, function, and standard of quality and performance required. It is not the intent of CITZ to exclude other materials, equipment, or processes to limit competition in bidding. Therefore, unless the proprietary named device referred to in the standards is a major system component and is followed by the words "no equal" indicating that no substitution is permitted, materials or equipment of other manufacturers will be considered by CITZ for substitution. CITZ major system components are manufacturer specific and substitution will not be permitted.

.2 Consideration will be given to a proposed substitute only when sufficient information is submitted to CITZ BTA'S for Security to determine that the proposed substitute material, equipment or process, is in fact equivalent in all respects to the materials, equipment or processes, named in these standards.

.3 Do not assume that the materials, equipment or process, will be approved as equal until the item has been specifically approved for this work through consultation with CITZ's Building Technology Advisors for Security (BTA).

1.6. Work with Others - Cooperation

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

.2 Security installation contractor(s) shall coordinate work with CITZ and their appointed representatives, to ensure alarm systems are installed, programmed, tested, commissioned and verified fully operational with SafeLink Central Monitoring Station; to the satisfaction of CITZ.

1.7. Documentation

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

a) All user and installation manuals.

b) As-built drawings.

c) All other forms and reports as required per this document. (i.e. load testing, etc.)

d) A printout of the monitoring company activity report that verifies full system testing.

e) Completed Letter of Conformance (Addendum 10.1)

f) Completed OPR Checklist (Addendum 10.2)

g) Device verification sign-off sheets.

h) Manufacturer's cut sheets for all devices.

i) All forms as supplied by WSI.

j) Electrical inspection permit and report.

k) Warranty Certificate.

l) Addendums and RFI's.

m) CMMS/Inventory Control Forms.

n) Copies of any additional Government supplied forms.

.2 The contractor shall provide a list of individuals trained. (Contractor shall provide CITZ with a training attendance sign-off sheet. This sheet shall identify the site, time, and date).

.3 As-built drawings (CAD and PDF) must show location of all devices, controls, demark connection(s), panels, keypads, strobes and sirens. All zones and partitions shall be clearly identified in the drawings.

.4 Electrical panel circuit breaker shall be clearly identified and noted on all as-built drawings and security system panel covers.

.5 All documentation is to be submitted electronically to both Safelink, and the WSI-CMMS group at CMMS@bljc.com.

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 (unless otherwise specified) and shall be conducted at a time that is mutually agreeable to both the contractor and CITZ. List to be supplied with individuals trained and the date in which training occurred.

1.9. Warranty

.1 The warranty period with respect to the Contract, is to be a minimum of one (1) year parts and labor 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 (at no additional cost) to keep the system fully 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).

2. Purpose

For the purposes of these standards, CITZ shall mean Ministry of Citizen' Services or their appointed representative BGIS WORKPLACE SOLUTIONS INC. herein referred to as WSI. Note that all approvals must be by CITZ (not WSI). Any deviation from these standards must be completed in consultation with CITZ Building Technology Advisors for Security (BTA).

The purpose of this Security Standard is to document the specific goals and objectives of CITZ to define the major system software and hardware components that comprise the Security Management System (SMS), and to provide general design guidelines for integration of the SMS into new and existing buildings and site development projects throughout CITZ facilities. The principal goal of this document is to provide consistent design and implementation standards for the integration of physical electronic security devices. The design standards included in this document describe system device performance requirements for each of the applicable devices that may be included within a specific project.

The SMS is comprised of three major electronic security sub-systems.

- Building Intrusion Alarm (BIA)
- Access Control System (ACS)
- Video Surveillance System (VSS)

Each of these sub-systems is comprised of command/control hardware, software, and field devices. The command/control hardware and software are standardized as to provide CITZ with a single, unified operational platform for physical security management. Security field devices will be designed and specified on a project specific basis throughout the course of the execution of new and retrofit construction.

Not all of the devices described in this document will necessarily be included in each project. It is the responsibility of the design team assigned to each project to use the security standards and protocols in this document to develop the appropriate deployment strategy and device requirements for their particular project.

2.1. Building Intrusion Alarms

The Building Intrusion Alarm (BIA) is primarily hardware based, and is a mandatory minimum requirement for securing any office, building, or other B.C. Provincial Government space. It is comprised of building alarm panels, with associated field devices. These systems are identical to commercial and residential "burglar alarm systems" in that the panel receives alarm signals from various field devices and, when the system is armed, transmits that alarm information to a central alarm monitoring station (Safelink).

2.2. Access Control Systems

The Access Control System (ACS) is the core platform of the SMS. It is a software based system that provides command and control functionality for the access control doors and associated hardware, stores access control credentials and privileges, provides the primary graphical user interface for monitoring and managing electronic security events and alarms, and serves as the central repository for system events than can be used for investigative and administrative purposes.

2.3. Video Surveillance Systems

The Video Surveillance System (VSS) is a software based sub-system that operates at a deep integration level with the SMS. The software provides configuration, control, monitoring and recording management of digital cameras, and digitally encoded signals from analog cameras. All cameras are recorded within the system and video is to be stored for a minimum of 14 days unless otherwise specified. The system is network based and is substantially reliant on the network for transmission of video data.

3. Security Systems

3.1. Operational Requirements

.1 Electronic security systems installed in Ministry of Citizen' Services (CITZ) facilities shall operate on a 24-hour basis throughout the year.

3.2. Power Requirements

.1 The security systems shall be hard-wired (i.e. no plug-in type transformers) to dedicated, non-switched electrical circuits and the circuit #'s must be clearly identified on both the electrical panel directory and security device panel.

.2 Each system shall have sufficient power supply to operate the system. The manufacturers' recommended power for the system shall be less than 80% of the power supply rated power output.

.3 All security systems power supplies are to be supervised by the BIA.

.4 Unless otherwise required, 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. (All batteries shall be a minimum 7 amp hour). Contractor is responsible for performing and providing, load calculations.

.5 Each system shall undergo a minimum (1) one minute load test with all devices, including sirens and strobe lights. Documentation of this testing must be provided.

.6 UPS equipment should be rack mounted and supervised by the BIA. UPS should provide a minimum 30 min of backup power and be integrated to signal the attached equipment to shutdown properly in the event of a power failure.

3.3. Physical Door Hardware

.1 Exterior Doors: full length astragals and NRP (non-removable pin) hinges are required.

.2 Interior Doors: astragals and NRP (non-removable pin) hinges are required for all doors to protected space.

3.4. 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 (CSA) or recognized approved equivalent. All materials including hardware and software being supplied, shall be new and of the latest version or production model.

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

3.5. Systems Hardening

.1 Systems must be setup in a protected network environment or by using a method that assures the system is not accessible via a potentially hostile network, until it is secured.

.2 Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures.

.3 Services, applications and user accounts that are not being utilized, should be disabled or uninstalled.

.4 Methods should be enabled to limit connections to services running on the host, to only authorized users of the service. Software firewalls, hardware firewalls, and service configuration are a few of the methods that may be employed.

.5 Methods should be taken to disable network, USB, and other ports that are not being utilized.

.6 Services or applications running on systems manipulating personal data, should implement secure (encrypted) communications.

.7 Systems will provide secure storage for data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to, encryption, access controls, file system audits, physically securing the storage media, or any combination thereof deemed appropriate.

.8 Strong password requirements will be enabled; as technology and operational procedures permit.

3.6. Backups

.1 System administrators should establish and follow a procedure to carry out regular system backups.

.2 Systems administrators must maintain documented restoration procedures for systems and their data.

.3 Backup media must be secured from unauthorized physical access. Backup media must be stored on-site, and must be encrypted or have a documented process to prevent unauthorized access.

3.7. Change Management

.1 There must be a change control process for systems configuration. This process must be documented.

.2 System changes should be evaluated prior to being applied in a production environment. Patches must be tested prior to installation in the production environment if a test environment is available. If a test environment is not available, the lack of patch testing should be communicated to CITZ, along with possible changes in the environment due to the patch.

4. INTRUSION ALARM SYSTEMS

4.1. General

.1 The protected space shall be provided with a complete intrusion alarm system (BIA). Intrusion protection shall be provided by way of door and window position sensors and dual technology motion detectors (Note: glass break detectors may only be used as an additional layer to motion detection, for higher security areas). The BIA is designed to detect unauthorized entry into protected spaces. The system shall conform to the requirements of this document.

.2 Wherever low voltage lighting control systems are used; provide an interface between the BIA and the low voltage lighting control system so that the intrusion alarm system can be used to switch off selected lighting and plug loads during unoccupied hours. Whenever the BIA is armed (either manually or automatically) a control signal shall be sent from the alarm panel to the lighting control panel to switch "off" the selected loads. When the BIA is disarmed (either manually or automatically) a control signal shall be sent from the alarm panel to the lighting control panel to switch "on" the selected loads.

.3 The BIA may be divided into separate partitions (areas).

.4 The BIA 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).

.5 Home-run all devices to the alarm panel - do not gang, daisy chain, or group devices unless otherwise authorized in writing by CITZ.

.6 Unless otherwise specified, system shall be integrated with the ACS to disarm when a valid access credential is used (first person).

.7 Each partition of the BIA will have as a minimum, the following devices:

a) Full Message LCD keypad

b) Door Position Sensor (all entry/exit points and telecommunication closets).

c) Motion Detector (all accessible perimeter windows, offices and entry/exit doors - including telecommunication closets)

d) Siren

.8 All devices (including control and expander panels) shall be supervised with tamper switches and end-of-line resistors (EOLR).

.9 EOLR shall be installed at the end devices – not in the panel.

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

.11 Installation includes the provision of all field equipment, mounting hardware, wiring, cable, terminations and I/O modules required to support the various alarm points and/or alarm systems. Installation also includes any related programming, setup and testing of system functionality; including all field devices.

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

a) All entry doors to be equipped with door position sensors.

b) At least one (1) motion detector to be installed in each telecommunications closet. To be determined by space/detection requirements.

.13 All environmental alarms are to be programmed as 24-hour zones, and activated for continuous monitoring.

.14 Control Panels shall have labels attached to the front indicating the equipment, applicable zone numbers, electrical circuit, and the date the battery was installed.

.15 If used, terminal strips must be mounted securely within an approved enclosure. The enclosure must be tampered as a supervised zone on the intrusion panel.

.16 Standard of Acceptance:

- DSC 4020, 1832 and 1864 series (most current versions);
- Bosch G Series;
- "No Equal"

4.2. Programming

.1 The contractor shall be responsible for all programming of the system. This includes all user codes, zone definitions, and establishing a connection to the CITZ monitoring station (Safelink).

.2 CITZ 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:

a) User code required to bypass zones

b) Daily test transmission (after 00:01 – 5:00, but not on the hour)

c) Bell time-out shall be set at 4 minutes

d) Home-away enabled

e) Disable reporting of partition opening/closing. All reporting is to be by user only.

f) Unless otherwise directed, all panels shall be programmed to auto-arm at multiple intervals throughout the unoccupied times.

g) Remote download access enabled

h) Intrusion panel upload codes to be changed from default and provided to Safelink.

i) Installer codes to be changed from default and provided to Safelink prior to upload.

j) The contractor shall not enable a contractor's lockout, and shall not program Forced Arming or Auto-Disarming without prior approval from CITZ.

.5 Upon completion of programming, the installer shall initiate an upload of the panel programming to Safelink (CITZ authorized monitoring agent).

.6 Confirmation of all alarm signals and successful system upload must be documented with verification number, provided by Safelink.

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

4.3. Monitoring

.1 CITZ 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 CITZ. Methods below are listed in order of CITZ preference:

a) Primary network connection, with secondary cellular backup;

b) Primary network connection, with secondary cellular backup and third telephone communicator backup.

c) Primary network connection, with secondary telephone backup;

d) Primary telephone connection, with secondary network backup;

e) Primary telephone connection, with secondary cellular backup;

f) Primary telephone connection only - with CITZ approval.

.3 All options must be set up with a single primary reporting path. Backup communicators will operate as secondary and third paths if the primary communication fails.

.4 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.

.5 All telephone jacks used for alarm/security systems shall be wired to USOC RJ31X industry standards. All jacks shall be installed with a tamper loop (ahead of the demark block), and shall clearly show the phone # for the jack.

.6 Monitoring is arranged by WSI and they shall issue all phone numbers required for monitoring and downloading. All intrusion alarm systems utilizing telephone communications shall be connected to analog telephone lines - no UC (Unified Communications).

4.4. Keypads

.1 No global operation for keypads - each partition must have its own keypad.

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

.3 All keypad mounted panic buttons shall be disabled.

.4 All keypads shall have "Quick Arming" enabled. For example: (* then 0)

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

4.5. Network Alarm Communicators

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

.2 Network alarm communicators shall connect to the Building Utility Subnet (BUS).

.3 Communicator minimum specifications:

a) 128-bit AES encryption

b) Low network bandwidth requirements

c) Compatible with 10/100BaseT networks

d) Reports events to at least 2 different receiver IP addresses

e) Programmable through dedicated software

.4 Standard of Acceptance:

- DSC TL-250;
- Bosch G Series Panels with built in IP Communicator;
- "No Equal"

4.6. Sirens, Strobes, and other Notification Devices

.1 All notification requirements include offices and/or rooms that may have the ability to close their doors. Please make sure notification (db) levels are compliant within these spaces.

.2 The system shall include sufficient interior alarm sirens to provide an audible (15db above average ambient sound level (NFPA 72)) alarm warning throughout the protected space. The contractor shall supply any additional sirens as required, to meet the above criterion. (Interior sirens to be minimum 15 watts)

.3 A separate siren shall be installed for each partition.

.4 All sirens and strobes to be on an isolated and supervised, power supply.

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

.6 An exterior strobe (blue) shall be installed for all systems without 24 hour security staff; location to be decided in consultation with CITZ (strobe may be mounted inside a window within the protected space - provided the strobe is visible from the exterior of the building).

.7 Strobe shall be latched, so that the panel must be reset to turn it off. (The strobe will provide staff with a visual warning that the alarm system has/had been activated.)

.8 An interior 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 (10db above average ambient sound level (NFPA 72)) throughout the protected space. The contractor shall supply any additional sound devices should the space require them, to meet the above criterion.

.9 Some perimeter doors may be designated as "Emergency Exit Only" and will be equipped with door position sensors. Upon violation of an emergency exit door, a local sounder should be activated. The sounder should continue to sound until expiration of the pre-determined software dwell time. Horn should deliver a minimum +/- 90 peak db.

.10 Standard of Acceptance:

- Interior Sirens – Honeywell WAVE-2F and 700 Series
- Exterior strobe/siren (blue) - Amseco SSX 52SB
- Exterior siren – Amseco SSX 52
- Strobe (blue) – Amseco SL-401

4.7. Auto-Arming and Cancellation

.1 CITZ requires the BIA (Building Intrusion Alarm) to auto-arm at specified times of day as per 4.2.4.f

.2 Whenever the protected space has the potential to be occupied at the scheduled BIA arming times, a method of cancellation must be provided within 15M of any occupied area.

.3 Cancellation methods include the following;

a) Building Intrusion Alarm Keypad
b) Access Control System Reader
c) Cancellation Button (blue mushroom style pushbutton).

.4 Please reference section 4.6.8 for arming notification requirements.

4.8. Motion Detectors

.1 Motion detectors should be used to provide internal area alarm detection on a time scheduled basis.

.2 Motion detectors should utilize both microwave and passive infrared technology to reduce false alarms.

.3 All motion detectors shall be installed and field-adjusted as per manufacturer's specifications for full coverage pattern of the protected spaces.

.4 360° detectors may be only be considered after consultation with CITZ.

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

.6 Standard of Acceptance:

- Bosch Commercial and Professional Series;
- Optex DX Series;
- Honeywell DT series

4.9. Glass Break Detectors

.1 Glass break detectors shall only be used as an additional layer to motion detection for higher security areas, and/or when otherwise specifically required by CITZ.

.2 Glass break detectors should provide low and high frequency detection to reduce the likelihood of false alarms.

.3 Glass break detectors should be zoned within rooms when complete glass protection requires multiple devices.

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

.5 Standard of Acceptance:

- GE SR-5815NT;
- Honeywell FG1625

4.10. Door/Window Position Sensors

.1 Every door which leads to the protected space shall be fitted with a commercial grade steel door position sensor.

.2 All grade level or easily accessible opening windows shall be equipped with a window position sensor.

.3 All door position sensors shall be installed at the top of the door, opposite the hinge side. Switches should be capable of initiating an alarm signal when the protected door is opened 1" on the latch side.

.4 All door and window sensors must be "wide gap" type to allow for false alarm minimization.

.5 All door and window sensors must be a minimum of 3/8" diameter. All sensors should be recessed, unless otherwise directed. If installed in wood or similar material, allow for expansion. Fill all voids with RTV silicone or equivalent.

.6 When surface mount sensors have been approved; they should have aluminum housings and be equipped with an armored cable jacket. Surface mount sensors should be mounted to the door header, with the associated magnet mounted to the door.

.7 Overhead door sensors should have aluminum housings, and be equipped with an armored cable jacket. Overhead sensors should be floor mounted with associated magnet surface mounted to the overhead door.

.8 When position sensors are used in conjunction with the ACS, door sensors must be double-pole-single-throw (DPST) to provide single circuit operation suitable for end-of-line supervision and connection to both the BIA and ACS.

.9 Standard of Acceptance:

- Sentrol 1078 series, Amseco AMS-25A/B, Amseco 38 Series;
- Overhead doors: Sentrol 2200 Series, Sentrol 2315A-L, Amseco ODC-59A/B

4.11. Cellular Backup

.1 Cellular units shall be installed in locations where there is a moderate to strong cellular reception.

.2 If a cellular back-up unit is installed, it must be equipped with its own power supply, which is sized to meet the maximum power requirements of the unit.

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

.4 The cellular unit shall monitor all signals including TLM (telephone line monitoring). These zones shall be coded and identified as coming from the cellular panel.

.5 Cellular unit must be capable of being monitored by SafeLink.

.6 Standard of Acceptance:

- DSC Model GS3060
- Uplinks Model 2550
- Bosch Connetix, ITS

4.12. Panic/Duress Alarms

.1 General

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

.2 Panic buttons to be strategically placed, or "hidden" from public view.

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

.4 All panic buttons located on movable furniture shall be connected using an RJ12 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

.1 Local panic systems will not be integrated into the main intrusion partition.

.2 When the panic alarm push button is pressed, a flashing light and chime (or other unique audible signal – not a siren) shall sound in a remote designated area (signal should not be within sight of push button location or view of the public).

.3 Local panic alarms must be programmed as have their zone options set to audible, to trigger chime notification(s) on alarm.

.4 Unless otherwise approved by CITZ, all panic alarms must be displayed individually on a LED keypad or appropriately sized annunciator panel.

.5 Standard of Acceptance:

- Multi-zone non-monitored panel: DSC Neo, PC1832, PC4020; Bosch G Series
- Annunciator panels (16 + zones or more): DSC PC4632, PC4664
- Panic button: Potter HUB-M (non-latching), HUB-2B (Latching LED)
- Wall Mount Panic Button: Sentrol 3045 (non-latching LED)

.3 Monitored Panic Alarm Systems

.1 Unless otherwise specified, the panic alarm system shall be a separate, monitored, standalone partition.

.2 Each panic alarm must be on its own dedicated zone and send a "24 Hour Panic" alarm to the central station when activated.

.3 CITZ and the client are to be consulted as to whether or not monitored panic buttons will also report locally.

.4 Wireless Panic Alarm Systems

.1 Wireless panic alarms shall only be installed in consultation with CITZ BTA's for Security.

5. ACCESS CONTROL SYSTEMS

5.1. General

.1 Access Control System (ACS) shall be installed within the protected space based on client requirements. Card readers, electric locking devices, door position and request-to-exit sensors, astragals and NRP (non-removable pin) hinges, shall be installed at all designated entry doors to the protected space including stairwell doors and points of public access. If an elevator is used to directly access the protected space, the ACS shall also be used to control the movement of the elevator on a floor by floor basis.

.2 The ACS shall be capable of expanding to allow for a minimum of 20% additional card readers.

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

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

.6 The ACS shall record all door held open/forced open events and shall be capable of providing an audible alarm and contact output for these conditions.

.7 The ACS shall include all new computer hardware, peripherals and software necessary to operate the system as designed, including the recording of all system event history. Materials shall meet or exceed manufacturer's requirements.

.8 The ACS shall be capable of generating a variety of historical reports which can be outputted to a computer screen and/or printer. The system shall allow the user to make changes to all system parameters including access cards, groups, levels, and schedules.

.9 The ACS shall not be dependent on the computer/server for its operation. That is, the access control panels shall 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 CITZ.

.11 Standard of Acceptance:

- Kantech Entra-Pass Special Edition. (Global Edition when required)
- Kantech Main Controller to be KT400; sub-controllers to be KT1 (KT100, 200, and 300 are no longer approved for use)
- "No Equal"

5.2. Proximity Readers

.1 All access controlled doors are to be secured with HID multiCLASS SE readers.

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

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

.4 Exterior card reader shall be weather proof, designed for outdoor applications and installed on 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 All readers must be tamper protected with either supervised optical and/or physical tamper switches.

.8 Standard of Acceptance:

- HID multiCLASS SE 2.4 GHz, 13.56 MHz & 125 kHz (Mobile Ready)
- "No Equal"

5.3. Request-to-Exit (REX)

.1 Wherever feasible, door hardware with integrated request-to-exit functionality is the preferred method of CITZ.

.2 Request to Exit (REX) motion sensors are to be used where door hardware REX functionality is not applicable. (Push button request-to-exit devices are not approved).

.3 REX devices shall be configured to allow egress through monitored doors while shunting door position sensor (upon activation) to prevent forced door alarms. REX device shall not unlock door(s).

.4 The REX motion detector shall have a built-in buzzer to locally annunciate "door forced" alarms and "door held open" warnings.

.5 REX devices must be tamper protected and supervised by the BIA or ACS.

.6 Standard of Acceptance:

- Kantech T-Rex
- Honeywell IS310/320

5.4. Electronic Locks

.1 Hardwired locks should be electrified mortise, cylindrical, strike, rim device, and/or exit device. All locking devices must meet CITZ requirements as well as the building, fire, and electrical code requirements of all AHJ (Authorities Having Jurisdiction).

.2 Locks shall be provided with appropriate wire transfer or electrified door hinge, which must be cabled on the secure side of the door.

.3 Unless otherwise directed by CITZ, electric locks shall fail "secure".

.4 All electric strikes shall be 12/24VDC, and receiver power from a dedicated power supply.

.5 Standard of Acceptance:

- Rutherford, Securitron, Folger Adam, HES
- Wireless lock solutions do not meet CITZ standards and are not approved for use.

5.5. Emergency Door Release

.1 Emergency Door Release (EDR) shall be in the form of door hardware as required by applicable building codes (e.g. crash bar).

.2 EDR should include a pneumatically controlled adjustable (2-60 seconds) time delay reset when delayed egress is required.

.3 EDR should include a DPST dry relay switch with one pole hardwired to locally interrupt power and the other pole hardwired to the ACS and configured as a hardwired input.

5.6. 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 ACS.

.3 The selector switch will be clearly labeled "Unlocked" and "Locked".

.4 Standard of Acceptance:

- Camden CM 190

5.7. 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 ACS.

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

.4 Standard of Acceptance:

- Camden CM 7000 Series

6. Intercom systems

6.1. Audio Intercom

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

.2 The client may elect to have the intercom interfaced with the ACS 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

6.2. Video Intercom

.1 The video intercom unit shall be installed on the exterior, 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 ACS so that they can remotely release the door. The contractor is responsible for all interfacing between the various systems.

.3 Standard of Acceptance:

- Aiphone AX, JF, JK, JP and KB Series

7. VIDEO SURVEILLANCE SYSTEMS

7.1. General

.1 The Video Surveillance System (VSS) 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://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/real-estate-space/video_surveillance_policy.pdf

.2 All new video surveillance systems shall utilize an NVR (server) and IP Cameras.

.3 Required camera resolutions are to be identified in drawings as Story Board, Recognize, or Identify as shown in table 7.2.1.13.

.4 Where the VSS manufacturer requires a camera in the system to be licensed, these licenses should be specified within each project design to accommodate the cameras specified within that particular project.

.5 VSS is to be on a separate, standalone network and will not be connected to the government network. Cameras shall not be monitored at any off-site location.

.6 The VSS shall include all equipment necessary for a fully functioning system.

.7 Contractor shall perform all calculations to ensure the systems, hardware and networks meet the operational requirements. Including but not limited to: recording parameters, throughput, number of cameras, and the number of workstations.

.8 VSS shall be designed and installed by certified personnel (industry and/or manufacturer).

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

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

.11 Where IP network cameras are installed, wiring shall be in compliance with EIA/TIA 568/569 Standards.

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

.13 VSS (including all peripheral hardware) shall be protected from lightning and power surges.

7.2. Surveillance Cameras

.1 General

.1 It is the preference of CITZ to utilize IP cameras (operating on POE) with NVR's, rather than analog solutions. However, if an analog solution needs to be considered, CITZ consultation with their BTA's for security, is required.

.2 Unless specified otherwise, all cameras shall incorporate indoor/outdoor enclosures with vandal resistant domes constructed of high impact polycarbonate material; plenum rated back boxes, UV resistant, smoked, optically clear, acrylic lower dome(s) with a maximum of f/0.5 light loss, and tamper resistant hardware.

.3 Camera should be as discreet as possible. Color, finish, and form factor should be closely coordinated with the project architect to balance the use and function while maintaining the desired aesthetic.

.4 Cameras should use a high resolution, progressive scan, 1/3" or greater CMOS imager with varifocal/auto-iris lens, and a range applicable to capture the desired field of view.

.5 Resolution of cameras should comply with the pixel-per-foot table below. Unless otherwise identified, all cameras should meet the pixel-per-foot requirements for the "Storyboard" view.

.6 Interior cameras should be suitable for interior installation environments.

.7 Exterior cameras should be suitable for exterior installation environments and should be provided with integral heaters/blowers/seals/etc. necessary to operate in the applicable exterior environment. The camera's operating temperature range shall be -40° to 50° Celsius (-40° to 122° F).

.8 Under no circumstances shall an empty housing or non-operational (dummy) camera be installed.

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

.10 IR illumination shall be used as required, to ensure that the area of interest is illuminated to the camera's minimum illumination requirements.

.11 Wide Dynamic Range (WDR) shall be used on all exterior cameras and locations with direct sunlight, and/or vehicle headlights within the field of view.

.12 Camera resolutions shall meet or exceed the minimum requirements for each type of scene as identified in the following table:

Table 7.2.1.13: Maximum Horizontal width (ft.) of field of view at area of interest.

	4CIF	1MP	2MP	3MP	5MP
Story Board	35	64	80	102	130
Recognize (Good Conditions)	18	32	40	51	65
Identify (Good Conditions)	7	13	16	20	26

Story board: used to provide overall context and view of a larger area.

Recognition: used to determine if movement is from a person, animal or object.

Identification: used to identify a person.

* For cameras above 5MP provide calculations showing pixels per foot at area of interest.

.14 Analog Cameras:

.1 Analog cameras are no longer accepted without consultation from CITZ BTA's for Security. Wherever possible, analog cameras should be replaced with IP cameras and network cabling.

.15 IP Cameras:

.1 Cameras shall use H.264 (or newer) compression with a maximum 2 second key-frame interval.

.2 All cameras must be POE capable, unless otherwise specified.

.3 All cameras are to have the default login information changed. Information is to be documented and submitted along with the shop drawings.

.4 All cameras are to be capable of being controlled and programmed through the VSS.

.5 Standard of Acceptance:

- IP Cameras: Axis, Avigilon, Bosch, Panasonic, Sony

7.3. Recording and Retention

.1 Unless otherwise specified, new video surveillance systems shall utilize an NVR for recording video.

.2 Unless otherwise specified, cameras shall record at the maximum resolution available, with a per camera parameter of 1fps recording 24/7 / 15fps on motion with a 10 second pre and post event.

.3 Video recordings shall be retained for a period of no less than 14 calendar days.

.4 The VSS shall be capable of managing all existing and new cameras (including Pan/Tilt/Zoom, pre and post recording of motion, adjustable frame rates, sequencing, and multiplexing).

.5 The VSS shall have the ability to switch frame rates on event without experiencing any loss in video recording.

.6 The VSS and networks shall provide sufficient capacity to accept all cameras with 20% spare capacity (bandwidth and throughput) as required at time of installation.

.7 The VSS shall include all necessary licensed software (including operating system(s)). It will also have a time/date generator and alarm recording features.

.8 The VSS shall have the ability to record all images in a proprietary file format with forensic digital watermarking features.

.9 Video management software must be capable of extracting video in AVI format as well as the native file format with watermark. Native file format must include an embedded player. Player must not require installation or user privileges' to play video.

.10 The VSS must have the ability to output to a DVD/R and USB drive, and shall be complete with all programs and equipment required to view images. This may include workstation(s), kvm(s), keyboard(s), monitor(s), and mouse/mice.

.11 The storage hardware is to be mounted in a secure location as directed by CITZ. Contractor shall coordinate final mounting location at site prior to installation. Security equipment shall not share racks and/or cabinets with other client hardware.

.12 Recording and network hardware shall utilize a UPS to provide a minimum of 30min backup power and filter AC (applicable to sites that do not have a central UPS). UPS must be integrated to allow the attached hardware to shut down in the event of a power outage. Hardware shall receive power from a central UPS where one is present.

.13 Whenever possible, the UPS should be rack mounted and connected to BIA as a 24hr supervisory alarm.

.14 Video management software must be fully programmed to provide suitable recording times (as per client requirements).

.15 Standard of Acceptance:

- NVR: Avigilon, Bosch
- VMS: Avigilon, Genetec
- Servers: Dell, HP

7.4. Video Surveillance Network

.1 The network shall be capable of supporting an IP Surveillance System. This includes bandwidth, throughput, QoS, security, network services, and virtualization.

.2 The network must be an isolated LAN that is not connected to the BC Government network (SpanBC), ISP, or any other 3rd Party network.

.3 Unless otherwise stated the network shall not use any wireless technology. Any wireless considerations would need to be authorized through consultation with CITZ BTA's for Security.

.4 All network and other ports must be disabled if not in current use.

.5 The network components must meet or exceed the requirements as specified by the VSS manufacturer.

.6 The network shall be capable of QoS, Multicasting, Layer 3 routing and Layer 2 switching.

.7 Camera/Workstation cabling (CAT5e cable) shall be terminated on RJ-45 data jack receptacles at each location and modular jack patch panels at equipment closets and main equipment rack cabinets. Provide patch cords as required to connect cameras and interconnect switches at patch panels.

.8 Maximum length of CAT5e horizontal cable run shall not exceed 85 meters

.9 Where CAT5e UTP cabling exceeds 85 meters, Multimode fiber optic cabling shall be used instead with copper to fiber media converters.

.10 All servers, cameras, encoders, and workstations on the network will have DHCP reservations for IP addresses. A DHCP server shall be supplied and configured to provide IP address reservations based on device MAC addresses.

.11 All installer passwords, switch configurations, IP and MAC addresses, shall be turned over to the client at the end of the project and shall be included in the O&M manuals.

.12 Wherever possible, health monitoring and anomaly detection should be utilized and integrated within the VSS network for the monitoring and detection of events/alarms.

.13 Standard of Acceptance:

- Network Switches: Allied Telesis, Comnet, HP, Cisco

.14 Workstations

.1 All workstations must be located within a secured area with keyboard, mouse and monitor functionality back to the to the operator location.

.2 All workstations must meet or exceed the minimum requirements specified by the VSS.

.3 All VSS workstation(s) will include at least one (1) LCD monitor installed at designated operator locations.

.15 Monitors

.1 All monitors must meet or exceed the minimum requirements specified by the VSS.

.2 Spot monitors must not be connected directly from camera but rather connected as a feed from VSS workstation/head-end.

.3 Monitors shall be wall or desk mounted as per CITZ requirements.

.4 All monitors shall be LCD with DVI and HDMI connections, a minimum screen size of 21 inches, and a minimum 1280 x 1024 resolution.

8. PERIMETER INTRUSION DETECTION SYSTEMS

8.1. General

.1 Equipment for perimeter intrusion detection systems (PIDS) may consist of one or more of the following:

a) Perimeter beam systems

b) Fence vibration systems

c) Ground vibration (seismic) systems (in consultation with CITZ BTA's for Security)

d) Electromagnetic field systems (in consultation with CITZ BTA's for Security)

e) Video surveillance systems (VSS/PIDS Integration / in consultation with CITZ BTA's for Security)

f) Video surveillance analytics (in consultation with CITZ BTA's for Security)

g) Other (in consultation with CITZ BTA's for Security)

8.2. Perimeter Beam Systems

.1 Each beam tower shall be set up so that the alarm and tamper outputs are wired in series, with a separate environmental output for fog, etc.

.2 Unless otherwise specified, 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 are 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 is to be installed in appropriately sized plastic conduit (min. 20mm - 3/4"). All conduits to be buried to a minimum of 900 mm (36") Installation must meet code requirements of AHJ (authority having jurisdiction).

.10 All cabling to be of direct burial type and shall meet the manufacturer's specifications.

.11 AC power 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:

- Takex
- Optex Rednet series
- Sicurit Absolute Pro Series

8.3. Fence Vibration Systems

.1 The fence-mounted system shall detect vibrations from cut or climb attempts to the fence fabric and subsequently identify the point of intrusion to within 3 meters (10 ft.).

.2 The fence cable system zone configurations shall be based on the design criteria listed below:

a) Zones should not exceed 15 linear meters (50 ft.) in length for optimum video surveillance assessment.

b) Zones shall not extend around corners in perimeter fencing.

.3 The partitioning of the perimeter fence into detection zones shall be established in software after installation of the system and in consideration of site conditions. Considerations for zoning shall include the reduction of nuisance alarms and assessment advantages for patrol personnel.

.4 The fence system shall detect climbing intruders with a weight of 34 kilograms (75 lbs.) with a Probability of Detection (Pd) of 95% at a 99% confidence level.

.5 The fence system shall detect cuts to the fence fabric with a Probability of Detection (Pd) of 95% at a 99% confidence level.

.6 All fence vibration detection zones to be on a separate partition (i.e. - compound partition). This partition will be independent of all other alarm system partitions.

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

.8 Disarming the partition compound will shunt all designated zones.

.9 AC power for the fence vibration detection system will be a separate circuit, and the circuit # shall be identified at the perimeter beam system panel.

.10 Standard of Acceptance:

- Southwest Microwave

9. EXECUTION

9.1. Installation

.1 Whenever systems are being upgraded and/or installed, all abandoned cabling and devices must be removed.

.2 System(s) shall be installed in a manner that is consistent with the provisions and intent of the project specific Specifications and Drawings, the referenced Codes and Standards, and in accordance with equipment manufacturers' written Specifications and Instructions.

.3 Installation and service workmanship should be accomplished in a neat and professional manner, meeting best industry standards. The contractor is responsible for cleanup and disposal of all garbage and debris caused as a result of their work.

.4 Configuration and programming of all panels and devices associated with a specific project shall be included as a requirement within that project. All configuration and programming shall be coordinated with CITZ representatives and shall match the existing naming and classification schema.

.5 Contractor shall test and commission systems as fully operational and functional prior to turnover to the CITZ. CITZ 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 CITZ

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

a) Cable number

b) Source

c) Destination

.7 All security systems require dedicated non-switched electrical circuits based on systems power requirements. Electrical panel circuit number shall be clearly identified on all system panels and on as-built drawings

.8 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.

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

9.2. 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 are sufficient to meet requirements for power and control, on all equipment being installed for use with their system. Contractor shall provide any related calculations on request.

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

.5 Where IP cameras are installed, all wiring shall be compliant with EIA/TIA 568/569 Standards.

.6 All network cabling shall be supplied, installed, terminated and tested to fully meet EIA/TIA 568 Transmission Performance Specifications. Test report shall be included with the O&M Manual.

.7 Where access control readers are installed, readers must be cabled with 6 conductor shielded cable (reader), 22/4 (tamper), and 2/18TSP (future OSDP). Cabling must meet plenum requirements as per AHJ.

.8 Cables placed in underground ducts and conduit outside of buildings shall be rated for outdoor use with water blocking membranes, when applicable.

.9 No splices shall be permitted in the wiring except when approved through consultation with CITZ.

9.3. Secure 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 BIA, ACS and VSS, shall be mounted at locations designated in consultation with CITZ.

.2 All security systems must be installed on their own freestanding rack(s) or wall mounted cabinet(s). Security equipment shall not share any rack or cabinet with other client hardware.

9.4. Grounding and Bonding

.1 Ground all security equipment as per manufacturer's recommendations and per AHJ.

.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), Bonding Requirements for Telecommunications, and the most current version of the CEC.

9.5. Pathways

.1 All wiring or cable connected to any piece of security equipment, that is accessible to the public, shall be installed in conduit to provide both security and mechanical protection of the cable.

.2 Conduit connecting to field devices such as camera enclosures 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 to be filled less than 40% of capacity.

.3 When ceiling pathways are utilized, cabling and installation shall conform to EIA/TIA 569 – Pathways and Spaces.

.4 Security communication and power cabling shall be routed away from voice/data cables to prevent interference as per EIA/TIA 568/569 Standards.

9.6. Procedure for Activating and Commissioning Electronic Security Systems

.1 Installation of all electronic security systems and ancillary equipment shall conform to the CITZ Security System Standards.

.2 The consultant or engineer is responsible for performing an independent commissioning of the system. This must cover functionality testing of all components within the system.

.3 The consultant or engineer to sign off that the system meets the full requirements of the system design and standards. (See CITZ Technical Standards for Offices - Section 12 – Commissioning)

.4 On-site commissioning, and provision of all personnel and equipment necessary to perform these tests, should be inclusive to each project referencing work included in this standard.

.5 Commissioning should include operational verification and testing of all new and existing devices installed, modified, and/or associated with the scope of the project.

.6 Intrusion alarm system account numbers and receiver IP information shall be provided by Safelink monitoring station.

.7 The security installation contractor must download and complete the following forms from Safelink:

a) Alarm System Installation Report

b) Zone List

c) User List

d) Installation Checklist

- Safelink contact information:
  Phone #: 604-454-1085, email address: **data@paladinsecurity.com**

.8 Contractor Responsibilities

.1 The contractor shall ensure that each system is fully tested and conforms to CITZ Security Standards.

.2 The contractor shall ensure that all required information is provided and recorded on the Safelink forms to facilitate programming and activation of the account with Safelink.

.3 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.

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

10. APPENDIX

10.1. Letter of Conformance (example)

Letter of Conformance – Security

Project Name:

Instructions: Security Engineer or Designer/Consultant of Record circles the corresponding answer and initializes each clause below to confirm general compliance with each clause for the above project. Security Engineer of Record shall sign and sign this document indicating conformance.

Section A:

A.1	YES / NO	All security systems have been designed in compliance with CITZ's Security Standards and any deviations have been identified, recorded and approved by CITZ. Identify all deviations in Section B.
A.2	YES / NO	Complete intrusion alarm system and/or panic duress system has been tested and signals sent from all devices to SAFELINK. Contractor has provided a verification number indicating that SAFELINK has received all required information and alarm signals.
A.3	YES / NO	Complete Video Surveillance System (VSS) has been tested and all camera views have been verified and approved.
A.4	YES / NO	Complete Access Control System (ACS) has been tested and functionality meets CITZ's Security Standards, contract documents, and owner's requirements.
A.5	YES / NO	Record drawings have been received, reviewed and are complete
A.6	YES / NO	Training has been completed as per contract documents and owner's requirements.
A.7	YES / NO	All Security System products and installation are in general conformance with contract documents and shop drawings.

Section B: Deviations as per A1 above (attach additional sheet if required)

B1.

B2.

B3.

Security Engineer or Designer/Consultant of Record:

Name: *(print)* Company: _____

Signature: Date, 20_____

10.2. OPR Checklist (example)

Item #	System	Commissioning and Acceptance Testing Standard	Submission	Initial	Date Received
1	Security Design	a) CITZ Technical Standards for TI b) CITZ Security Standards	SER submit signed Letter of Conformance indicating all security system has been designed in compliance with CITZ Technical Standards for Tenant Improvements and CITZ Security Standards and deviations recorded.		
2	Intrusion and Duress Systems	1. CITZ Security Standards	SER submit signed letter of Conformance indicating complete intrusion alarm system and/or panic duress system have been tested and signals sent from all devices to SAFELINK. Contractor has provided a verification number indicating that SAFELINK has received all required information and alarm signals.		
3	Video Surveillance System	2. CITZ Security Standards	SER submit signed letter of Conformance indicating complete Video Surveillance System has been tested and all camera views have been verified and approved.		
4	Access Control System	a) CITZ Security Standards b) Contract Documents	SER submit signed letter of Conformance indicating complete Access Control System has been tested and functionality meets CITZ's Security Standards, contract documents, and owner's requirements.		
5	Record Drawings	a) CITZ Security Standards b) Contract Documents	SER submit signed letter of Conformance indicating record drawings have been received, reviewed and are complete		
7	O&M Manuals	a) CITZ Technical Standards for TI b) CITZ Security Standards	SER submit signed letter of Conformance indicating O&M manuals have been received, reviewed and are complete.		
8	Training	a) CITZ Security Standards b) Contract Documents	SER submit signed letter of Conformance indicating training has been completed as per contract documents and owner's requirements.		
9	Security Installation	a) CITZ Security Standards b) Contract Documents and Shop Drawings	SER submit signed letter of Conformance indicating all Security System products and installation are in general conformance with contract documents and shop drawings.		
General Notes	a. SER = Security Engineer or Designer/Consultant of Record. 3. b. If manufacturer has specific acceptance/commissioning testing requirements, they will be in addition to the standards listed above.				