PHYSICAL SECURITY STANDARDS

for Government of B.C. Facilities
1. PURPOSE

2. REFERENCE
   2.1. REFERENCE STANDARDS
   2.2. RELATED DOCUMENTS

3. CONDITIONS
   3.1. GENERAL
   3.2. MATERIAL SUBSTITUTIONS
   3.3. WORK WITH OTHERS - COOPERATION
   3.4. HANDOVER AND CLOSEOUT DOCUMENTATION
   3.5. TRAINING
   3.6. WARRANTY

4. CONSULTING AND DESIGN SERVICES
   4.1. QUALIFICATIONS
   4.2. LICENSING
   4.3. DESIGN REQUIREMENTS

5. GENERAL SYSTEM REQUIREMENTS
   5.1. OPERATIONAL
   5.2. POWER
   5.3. NETWORK CONNECTIVITY
   5.4. PRODUCTS
   5.5. SYSTEMS HARDENING
   5.6. BACKUPS
   5.7. CHANGE MANAGEMENT

6. INTRUSION ALARM SYSTEMS
   6.1. GENERAL
   6.2. AUTO-ARMING AND CANCELLATION
   6.3. DURESS / PANIC ALARMS
   6.4. TELECOM/DATA ROOMS AND CLOSETS
   6.5. PROGRAMMING
   6.6. DOOR/WINDOW POSITION SENSORS
   6.7. MOTION DETECTORS
   6.8. GLASS BREAK DETECTORS
   6.9. KEYPADS
   6.10. SIRENS, STROBES, AND OTHER Notification DEVICES
   6.11. NETWORK ALARM COMMUNICATORS
   6.12. CELLULAR BACKUP
   6.13. MONITORING

7. ACCESS CONTROL SYSTEMS
   7.1. GENERAL
   7.2. CREDENTIALS
   7.3. PROXIMITY READER
   7.4. REQUEST-TO-EXIT (REX)
   7.5. ELECTRONIC LOCKS
   7.6. DOOR POSITION SENSOR
   7.7. REMOTE DOOR CONTROL
   7.8. REMOTE DOOR RELEASE
8. VIDEO SURVEILLANCE SYSTEMS ................................................................................................................. 19
  8.1. GENERAL .................................................................................................................................................. 19
  8.2. SURVEILLANCE CAMERAS ....................................................................................................................... 20
  8.3. RECORDING AND RETENTION ............................................................................................................... 21
  8.4. VIDEO SURVEILLANCE NETWORK ......................................................................................................... 22
  8.5. WORKSTATIONS ....................................................................................................................................... 22
  8.6. MONITORS ................................................................................................................................................ 23
9. INTERCOM SYSTEMS ........................................................................................................................................ 24
  9.1. AUDIO INTERCOM ..................................................................................................................................... 24
  9.2. VIDEO INTERCOM .................................................................................................................................... 24
10. PERIMETER INTRUSION DETECTION SYSTEMS ............................................................................................. 25
  10.1. GENERAL ............................................................................................................................................... 25
  10.2. FENCE CUT, CLimb, TAMPER DETECTION SYSTEMS .......................................................................... 25
  10.3. PERIMETER BEAM SYSTEMS .................................................................................................................. 25
11. EXECUTION ..................................................................................................................................................... 27
  11.1. INSTALLATION ......................................................................................................................................... 27
  11.2. SYSTEM CONDUCTORS & CABLES ......................................................................................................... 27
  11.3. SECURE TERMINATION .......................................................................................................................... 28
  11.4. GROUNDING AND BONDING .................................................................................................................. 28
  11.5. PATHWAYS ............................................................................................................................................... 28
  11.6. COMMISSIONING OF ELECTRONIC SECURITY SYSTEMS ................................................................. 28
12. APPENDIX ......................................................................................................................................................... 29
  12.1. LETTER OF CONFORMANCE .................................................................................................................. 29
  12.2. OPR CHECKLIST ....................................................................................................................................... 30
1. PURPOSE

For these standards, RPD shall mean Ministry of Citizen’ Services, Real Property Division or their appointed Service Provider. Note that all approvals shall be by RPD (not Service Provider). Any deviation to these standards must be accompanied by written approval from RPD Security.

The purpose of this Physical Security Standard (PSS) is to ensure minimum requirements are met in the design, development, installation and management of security systems for the Government of B.C. These standards document the specific goals and objectives of RPD to define the major system software and hardware components that comprise the Government of B.C.’s Enterprise Security Management System (ESMS) and to provide design requirements for integration of the ESMS into new and existing buildings and site development projects.

The principal goal of this document is to provide consistent design and implementation standards for physical and electronic security devices throughout B.C. Government facilities.

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

- Intrusion Alarm System (IAS)
- 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 the Government of B.C. with a single unified operational platform for enterprise physical security management. Security field devices shall be designed and specified on a project specific basis throughout the course of the execution of new and retrofit construction.

Not all the systems or devices described in the PSS shall necessarily be included in each project. It is the responsibility of the design team (in coordination with the client) to build upon the minimum requirements of the standard to develop the appropriate deployment strategy, device and functional requirements for each project.

2. REFERENCE

2.1. Reference Standards

All materials, workmanship, installation practices and/or other activities, shall meet or exceed the following reference standards:

- CAN/ULC-S302-14 Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems
- CAN/ULC-S316-14 Standard for Performance of Video Surveillance Systems
- CAN/ULC-S318-96 Standard for Power Supplies for Burglar Alarm Systems
- CAN/ULC-S319-05 Electronic Access Control Systems
- British Columbia Building Code and Local Building Bylaws
- Work Safe B.C.
- All other applicable Federal, Provincial and Municipal laws, regulations, and bylaws.

2.2. Related Documents

- 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](http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/real-estate-space/video_surveillance_policy.pdf)
3. CONDITIONS

3.1. General

.1 This document shall not be altered in any way and must be included as a complete document.

.2 These standards apply to all space owned and leased by the Government of British Columbia that holds government assets, information, networks and/or personnel.

.3 All new work must comply with this document. Substantial work or reconfiguration to existing space shall require the upgrading of the entire security system(s) to the requirements of this document.

.4 Compliance with these standards does not imply a completely secure environment. Instead, these requirements shall be integrated into a comprehensive site security plan.

.5 An intrusion alarm is a mandatory minimum requirement for securing any office, building or other B.C. Government facility.

.6 All electronic security systems for government leased/owned space shall be managed solely by the Government of B.C. The use of landlord owned, and/or managed systems is acceptable for common areas of buildings only and must not provide access to government space.

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

.8 The General Contractor shall not Sub-subcontract any portion of the security work without prior approval of RPD Security. (e.g. from general to electrical to security)

.9 Contractor shall take necessary measures to maintain security and prevent unauthorized access to government space and information during the performance of any work.

.10 The Government of B.C. shall have complete control of the operation of the system(s) while the building is occupied by the government and/or its tenants.

.11 Security systems must not be connected to the Government of B.C.’s networks as per government policies and standards. The exception is the BUS (Building Utility Subnet).

.12 All security workstations, servers, controllers and other devices, are to be provided and maintained by a licensed security services provider and not by government entities (e.g. OCIO).

.13 Any remote access required for management of security systems, requires RPD Security approval.

.14 All equipment shall remain the sole property of the Government of B.C. and the installing company shall not retain any ownership and/or control on, or of, the system(s).

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

.16 All intrusion systems shall be configured to be managed (locally) onsite and shall be connected to the Government of British Columbia’s BUS (Building Utility Subnet) for alarm monitoring.

.17 All Government of B.C. intrusion alarm accounts shall be monitored by the Paladin Technologies monitoring station.

.18 Any exceptions or deviations to these standards (including the determination of equivalencies) shall be approved by RPD Security: PhysicalSecurity@gov.bc.ca

3.2. 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 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 RPD 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 shall be considered by RPD for substitution. Major system components are manufacturer specific and substitution shall not be permitted.

.2 Consideration will be given to a proposed substitute only when enough information is submitted to RPD to determine that the proposed substitute material, equipment or process is in fact equivalent in all respects to the materials, equipment or process defined in these standards.

.3 Do not assume that the materials, equipment or process shall be approved as equal until the item has been specifically approved for this work through consultation with RPD Security.

3.3. Work with Others - Cooperation

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

.2 Security installation contractor(s) shall coordinate work with RPD and their appointed representatives to ensure alarm systems are installed, programmed, tested, commissioned and verified fully operational with the Paladin Technologies monitoring station, to the satisfaction of RPD.

3.4. Handover and Closeout Documentation

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

.1 User/Installation Manuals.

.2 Addendums and RFI’s.

.3 As-built drawings (CAD and PDF) showing 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 A printout of the monitoring company activity report that verifies full system testing.

.5 Device verification sign-off sheets.

.6 Manufacturer’s cut sheets for all devices.

.7 Electrical inspection permit and report.

.8 Warranty Certificate(s).

.9 Completed Letter of Conformance (Addendum 12.1).

.10 Completed OPR Checklist (Addendum 12.2).

.11 All other forms and reports as required per this document.

.12 All documentation is to be submitted electronically to RPD Security: PhysicalSecurity@gov.bc.ca

3.5. 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 the client. The contractor shall provide a list of individuals trained via an attendance sign-off sheet. This sheet shall identify the site, time and date of training.

3.6. 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(s) shall include all company contact information including emergency after-hours support.

4. CONSULTING AND DESIGN SERVICES

4.1. Qualifications

.1 The consulting, design, engineering, and commissioning of all electronic security systems for the Government of British Columbia shall be by qualified personnel that shall:

\[.1\] Have ten (10) year of security experience, at least five (5) years of which shall have been directly related to the design/engineering of physical and electronic security systems.

\[.2\] Hold all applicable license categories as per the British Columbia Security Services Act regardless of any other professional designation (including P. Eng.).

4.2. Licensing

.1 Any entity performing security work for the Government of British Columbia shall have a security business license issued by the Registrar of Security Services.

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

4.3. Design Requirements

.1 Security items shall be shown on dedicated drawings (Div. 28).

.2 The following representations are required for review:

\[.1\] Intrusion Alarm, Access Control, Door, and Video Surveillance hardware schedules, as applicable.

\[.2\] Relative Field-of-View (FOV) drawings for all video surveillance applications.

\[.3\] It is the responsibility of the systems design team to identify (as part of the security drawings and specifications) the client’s functional requirements specific to each project.

5. GENERAL SYSTEM REQUIREMENTS

5.1. Operational

.1 Electronic security systems shall operate on a 24-hour basis throughout the year.

5.2. Power

.1 The security systems shall be hard-wired (no plug-in type transformers) to dedicated non-switched electrical circuits and the circuit #’s shall be clearly identified on both the electrical panel directory and security controller’s (inside) panel cover.

.2 Electrical breakers that control security systems equipment shall be identified as such and secured against tamper (lockout).

.3 Each system shall have enough 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.

.4 Security systems shall be protected by an Uninterruptable Power Supply (UPS) to provide a minimum thirty minutes (30min) of backup power to all security devices, when not protected by a generator. If protected by a generator, backup power shall be supplied until the generator comes online.

.5 All security systems power supplies and UPS equipment shall be supervised by the IAS.

.6 UPS equipment shall be integrated to signal the attached equipment to shutdown properly in the event of a power failure.
5.3. **Network Connectivity**

.1 All intrusion alarm systems shall be connected to the Government of B.C.’s Building Utility Subnet (BUS) for the reporting of alarms and require an iStore order.

5.4. **Products**

.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 comply with 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 unless otherwise specified.

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

5.5. **Systems Hardening**

.1 Systems shall 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 All operating system and application updates or security patches shall be installed expediently and consistent with change management procedures (Chapter 5.7).

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

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

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

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

.7 Systems shall 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 shall be enabled as technology and operational procedures permit.

.9 All controller, expander, power supply and other security systems related enclosures shall be tamper-protected and serviceable.

5.6. **Backups**

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

.2 System administrators shall maintain documented restoration procedures for systems and their data.

.3 Backup media shall be secured from unauthorized physical access. Backup media may be stored off-site but shall be encrypted and have a documented process to prevent unauthorized access.

5.7. **Change Management**

.1 All changes to systems configuration shall be logged and associated to individual making change.

.2 System changes, updates, and patches shall be tested prior to installation in the production environment, if a test environment is available. If a test environment is not available, this lack of testing shall be communicated to RPD.
6. INTRUSION ALARM SYSTEMS

6.1. General

.1 An intrusion alarm (IAS) is a mandatory minimum requirement for securing any office, building or other Government of B.C. space. The IAS is designed to detect unauthorized entry into protected spaces. The system shall comply with the requirements of this document.

.2 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 systems. Installation also includes any related programming, setup and testing of system functionality.

.3 Intrusion protection shall be provided by way of hardwired door and window position sensors, with dual technology motion detectors (Note: glass break detectors may only be used as an additional layer to motion detection for higher security areas).

.4 The IAS control panel shall have enough zone inputs so that each device shall be connected to a single zone (double doors may be grouped as a single zone) and be home-run to the intrusion panel. Do not gang, daisy chain, or group devices.

.5 The IAS may be divided into separate partitions (areas).

.6 Each partition of the IAS shall have as a minimum the following devices:

   .1 Keypad
   .2 Door Position Sensor (all entry/exit points)
   .3 Motion Detector (covering all accessible perimeter windows, offices and entry/exit doors)
   .4 Siren

.7 Control panels shall have labels attached to their inside front covers indicating the equipment, applicable zone descriptors, electrical circuit, and date the battery was installed or last maintained.

.8 All intrusion detection devices shall be supervised with tamper switches and end-of-line resistance (EOLR). EOLR shall be installed at the end devices – not in the panel.

.9 Wherever low voltage lighting control systems are used; provide an interface between the IAS and the low voltage lighting control system so that the intrusion alarm system can be used to switch on and off selected lighting and plug loads. Whenever the IAS 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 IAS is disarmed, a control signal shall be sent from the alarm panel to the lighting control panel to switch “on” the selected loads.

.10 All environmental alarms shall be programmed as 24-hour zones and activated for continuous monitoring.

.11 If used, terminal strips shall be mounted securely within an approved enclosure. The enclosure shall be tamper-protected and monitored as a supervised zone on the intrusion panel.

.12 Standard of Acceptance:
   
   - DSC Maxsys
   - Bosch B and G Series
   - “No Equal”

6.2. Auto-Arming and Cancellation

.1 Intrusion alarms shall auto-arm at multiple times (min. 4) during evenings and weekends. The auto-arming schedules must be performed by the IAS.

.2 Recommended auto-arming times are 6pm, 8pm, 10, 12am (M-F) and 10am, 2pm, 6pm, 9pm (S-S). Requires client discussion to develop a schedule that compliments the operational requirements of each location. The
intention is to start auto-arming shortly after the space is typically vacant. The annunciation and cancellation methods are to enable easy management of this process should the operational needs change intermittently.

.3 Users shall quick-arm intrusion systems upon exit, with the auto-arming serving as a backup to this process.

.4 An interior, audible auto-arming warning shall be provided as per Chapter 6.10.8.

.5 A method of canceling the arming during the audible warning period shall be provided within 15M of any potentially occupied area(s). A momentary switch shall be used to provide this method of cancellation.

.6 Annunciators and cancellation devices shall be located within logical proximity to one another to facilitate ease of use.

.7 Standard of acceptance:
   - Momentary Switch: Camden CM-7000 Series (w/ green button and labelled, “hold for 2 seconds to cancel auto-arm”)
   - Annunciator: Piezoelectric Speaker (pulse)

6.3. Duress / Panic Alarms

.1 General
   .1 All public facing offices shall have monitored panic/duress initiating devices.
   .2 Panic alarms shall be activated by hardwired devices only. Wireless panic alarms require consultation with RPD Security, prior to implementation.
   .3 All panic alarm devices located on movable furniture shall be connected using an RJ12 wall jack and a telephone patch cord to the jack.
   .4 All panic alarm devices (and any associated wall jacks) shall be clearly identified by a machine printed label or professional method.
   .5 When the panic alarm is activated, a flashing blue light and chime (or other unique audible signal – not a siren) shall sound in designated area(s). Signal shall not be within sight of panic initiating location or view of the public, to mitigate the potential of escalation because of the alert.
   .6 Panic alarms shall be displayed on LED keypad(s) or appropriately sized annunciator panel(s) to simultaneously display all activated alarms.
   .7 Panic Alarm systems shall be a standalone monitored partition of the intrusion alarm. Each panic alarm shall have a dedicated zone and send a “24 Hour Panic” alarm to the central station when activated.

.2 Standard of Acceptance:
   - Annunciator panels (16 + zones or more): DSC PC4632, PC4664
   - Panic Devices: Sentrol 3045 (both under counter and wall mount applications)

6.4. Telecom/Data Rooms and Closets

.1 Telecom/data rooms and closets shall be included in the main office intrusion alarm partition when located within this protected space. Telecom rooms and closets that reside outside of the protected space (e.g. common areas, etc.) shall be protected by dedicated partition(s) of the office intrusion alarm.

.2 Each telecom room or closet to have the following minimum intrusion alarm equipment:
   .1 All entry doors to be equipped with door position sensors.
   .2 A minimum of one (1) motion detector. Additional motion detectors may be required as determined by space.
   .3 Intrusion alarm keypad (if required to be on its own partition).
6.5. **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 Paladin Technologies monitoring station.

.2 The client shall supply the contractor with all access codes to be programmed into the alarm system.

.3 When programming is managed by non-government entities, the names of individuals shall be redacted from the security systems. The use of user #’s shall replace user/staff names for these systems. The user #’s shall correlate to a master spreadsheet owned and managed by the client/tenant.

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

.5 The contractor shall program the following:

   .1 User code required to bypass zones (no forced bypass). Auto-arming may use a code with forced bypass privilege.

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

   .3 Bell time-out shall be set at 4 minutes. All strobes to be latching until reset.

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

   .5 Automatic disarming is not allowed under any circumstance.

   .6 Remote download access enabled.

   .7 Intrusion panel upload codes to be changed from default and provided to Paladin Technologies monitoring station.

   .8 Installer codes to be changed from default and provided to Paladin Technologies monitoring station prior to upload.

   .9 The contractor shall not enable a contractor’s lockout.

.6 Upon completion of programming, the installer shall initiate an upload of the panel programming to Paladin Technologies (authorized monitoring station).

.7 Confirmation of all alarm signals received, with a report detailing the systems programming and configuration, shall be documented and provided by the contractor as part of the project document submittals.

.8 Once the system installation is deemed substantially completed, the contractor shall not access the system either physically or electronically without RPD consultation and written permission.

6.6. **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 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. Sensors shall be capable of initiating an alarm signal when the protected door is opened a maximum of 1” on the latch side.

.4 All door and window sensors shall be “wide gap” type to align with false alarm reduction strategies.

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

.6 Surface mount sensors shall be mounted to the door header with the associated magnet mounted to the door. All exposed cabling shall be protected.

.7 Overhead door sensors shall have aluminum housings and be equipped with an armored cable jacket.

.8 Overhead sensors shall be floor mounted with associated magnet surface mounted to the overhead door.
9. When door position sensors are used to monitor position for both the IAS and the ACS, sensors shall be minimum double-pole-single-throw (DPST) to provide single circuit operation, suitable for end-of-line supervision and connection to both systems.

6.7. **Motion Detectors**

1. Motion detectors shall be used to provide internal area alarm detection on a time scheduled basis.
2. Motion detectors shall utilize both microwave and passive infrared technology to reduce false alarms. 360° detectors may offer multiple modes of false alarm reduction versus microwave detection.
3. All motion detectors shall be installed and field-adjusted as per manufacturer’s specifications for the appropriate coverage of the protected spaces.
4. All motion detectors shall have LED’s disabled after initial testing is complete.
5. Standard of Acceptance:
   - Honeywell DT series
   - Bosch Commercial and Professional Series
   - Optex DX Series

6.8. **Glass Break Detectors**

1. Glass break detectors shall only be used when as an additional layer to motion detection for higher security areas, or when otherwise specifically required by RPD.
2. Glass break detectors shall provide low and high frequency detection to reduce the likelihood of false alarms.
3. Glass break detectors shall 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 specifications.
5. Standard of Acceptance:
   - GE SR-5815NT
   - Honeywell FG1625

6.9. **Keypads**

1. No global operations allowed for keypads. Each partition shall have at least one dedicated keypad.
2. All IAS keypads are to be full alpha-numeric. The exception is Panic/Duress systems (which utilize LED keypads and/or annunciators to display alarms).
3. All keypad mounted emergency buttons shall be disabled, unless otherwise directed by RPD.
4. All keypads shall have “Quick Arming” enabled. For example: (* then 0)
5. All keypads to be installed fifty-four inches (54”) above finished floor. An additional keypad may be installed at an appropriate height for these locations when addressing accessibility required for operation.

6.10. **Sirens, Strobes, and other Notification Devices**

1. The system shall include enough interior alarm sirens to provide an audible (minimum 15dB above average ambient sound level) alarm warning throughout the protected space.
2. 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.
3. The contractor shall supply any additional devices as required to meet the above criterion.
4. A separate siren shall be installed for each partition.
5. All sirens and strobes shall be on isolated and supervised power supplies.
6. All systems shall be programmed for a four-minute (4min) siren/bell duration.
A strobe (red) shall be installed to notify returning staff that an intrusion event may be in progress, and to assist responding authorities in identifying the location. The strobe shall be visible from the exterior, by an area(s) suitable for its intended purpose and be latched so that the panel must be reset to turn it off. An exception is made for sites that employ 24/7 security officers whom would provide an immediate response.

An interior audible warning shall be provided for a minimum of three (3) minutes when the system is arming, whether manually or automatically. The warning tone shall be different from the alarm siren sound, (siren pulse is not acceptable), and shall be heard (minimum 10dB above average ambient sound level) throughout the protected space. The contractor shall supply any additional sound devices shall the space require them to meet the above criterion.

Some perimeter doors may be designated as “Emergency Exit Only” and shall be equipped with door position sensors. Upon violation of an emergency exit door, a local sounder shall be activated. The sounder shall continue to sound until expiration of the pre-determined software dwell time. Horn shall deliver a minimum +/- 80dB peak.

6.11. Network Alarm Communicators

The contractor shall provide a network alarm communicator connected to the IAS for reporting alarms over the Government of B.C. Building Utility Subnet (BUS).

Network alarm communicator connections to the BUS require an iStore order and coordination.

Communicator minimum specifications:

1. 128-bit AES encryption
2. Low network bandwidth requirements
3. Compatible with 10/100BaseT networks
4. Reports events to at least 2 different receiver IP addresses
5. Programmable through dedicated software

6.12. Cellular Backup

Cellular units shall be installed in locations where there is a moderate to strong cellular reception. If acceptable reception cannot be found within the premise, an exterior antenna solution may be required.

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

Cellular unit shall 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).

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

Cellular unit shall be capable of being monitored by Paladin Technologies monitoring station.

6.13. Monitoring

The Government of British Columbia retains the right to monitor their alarm systems in the manner of their choosing and shall not be locked into any other monitoring arrangements because of alarm system installations.

Contractor shall provide connectivity (hardware & software) with monitoring station as directed by RPD. Methods below are listed in order of preference:

1. Primary network connection through the B.C. GOV Building Utility Subnet (BUS), with secondary cellular backup;
2. Primary network connection through the B.C. GOV Building Utility Subnet (BUS), secondary cellular backup, and tertiary telephone communicator backup (High Security Applications).
.3 All options shall be set up with a single primary reporting path. Backup communicators shall operate as secondary and tertiary paths, if the primary communication fails.

.4 If a telephone line is to be used as a communication path, the demarcation point shall be marked “Intrusion Alarm – DO NOT DISCONNECT without informing RPD”.

.5 Intrusion systems utilizing telephone communications shall be connected to analog telephone lines. No UC (Unified Communications) or VOIP (Voice over Internet Protocol). Jacks used for (line seizure) shall be wired to USOC RJ31X industry standards, be installed with a tamper loop (ahead of the demark block), and clearly show the phone # for the jack.

.6 Monitoring is arranged by RPD’s Service Provider and they shall issue all relative information required for monitoring and downloading.

Paladin Technologies Monitoring Station
1(800) 241-1122 or data@paladintechnologies.com
7. ACCESS CONTROL SYSTEMS

7.1. General

.1 Access Control Systems (ACS) may be installed within the protected space based on client needs, and the requirements of this document.

.2 Card readers, electric locking devices, door position and request-to-exit sensors, security astragals, and NRP (non-removable pin) hinges, shall be installed at all designated entry doors to the protected space including stairwells. 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, whenever possible.

.3 It is the responsibility of the licensed security services provider to provision and maintain all security related devices including workstations, servers, networking hardware, etc.

.4 The ACS shall allow for a minimum of 20% additional card readers.

.5 The ACS shall have the capacity of either: one (1) access card for every square 10 meters ($10m^2$) of the protected space, or the number of cards immediately required by the tenant plus 20%.

.6 For low security applications: The ACS may be integrated with the IAS to disarm when a valid access credential is used (first person in). Systems shall continue to operate independently in the event of integration failure (single factor authentication).

.7 For medium to high security applications: The ACS may not be integrated with the IAS to disarm when a valid access credential is used (first person in). For these applications users shall enter with access card and then utilize a unique code on the intrusion keypad to disarm the alarm (two factor authentication).

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

.9 The ACS shall record all door held/forced open events and provide an audible alarm and contact output for these conditions.

.10 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.

.11 The ACS shall generate 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.

.12 The ACS shall not be dependent on the workstation/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.

.13 Standard of Acceptance:

- Kantech EntraPass Special Edition (unless other Kantech version required)
- Kantech Controllers to be KT400 or KT1; (KT100, 200 and 300 are not approved for use)
- “No Equal”

7.2. Credentials

.1 The Government of B.C. is migrating towards HID iCLASS Seos as the preferred access control credential. The following requirements shall be implemented within each project:

.1 All credentials shall be HID iCLASS Seos + Prox (multiclass) to accommodate migration path. Wherever Prox credentials are not used by staff, please disable this functionality.
.2 Seos authentication shall be utilized on all new readers and wherever else possible (i.e. existing Seos capable readers).

.3 Credential may be card or key fob depending on client requirements.

.4 It is possible to integrate the credential with a landlord’s access control system to provide a one-card solution for tenants [refer to Chapter 3.1.6]. If there is a variant of the HID 500x series credential that offers iCLASS Seos and Prox, it is acceptable to have a 3rd protocol if provided to enable compatibility with the landlord’s technology. If not compatible, a second credential shall be provided by the landlord and used for base building access.

.5 Must not have any identifying information (e.g. address, ministry name, etc.) included or attached.

.2 Standard of Acceptance:
   - HID iCLASS Seos 510 Series
   - "No Equal"

7.3 Proximity Reader

.1 All readers shall be tamper-protected and monitored as a 24-hour supervised device by the IAS.

.2 All readers to be installed forty-six inches (46”) above finished floor, unless directed otherwise by RPD.

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

.4 A built-in sounder shall provide distinctive audible feedback when:
   - a card is read
   - access is denied
   - during door-ajar pre-alarm and alarm.

.5 Exterior card reader shall be weather proof, designed for outdoor applications and installed on watertight boxes. All exterior card readers shall include the optional IP65 gasket kit when installed.

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

.7 Wherever access control readers are installed, readers shall be cabled with a minimum 18/6 shielded cable (reader), 22/4 (tamper), and 18/2 TSP (Future OSDP).

.8 Mullion sized readers may be used only in locations with limited mounting space or when specifically requested by RPD.

.9 Standard of Acceptance:
   - HID multiCLASS SE RP40, RPK40, RP10: with Open Source Device Protocol (OSDP);
     - Bluetooth Mobile Ready (not enabled); with support for 13.56 MHz & 125 kHZ credentials;
     - with connected Optical Tamper (monitored by intrusion alarm as per 7.3.1).
   - "No Equal"

7.4 Request-to-Exit (REX)

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

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

.3 The REX shall have a built-in buzzer to locally annunciate “door forced” alarms and “door held open” warnings.

.4 REX devices shall be tamper-protected and supervised by the IAS or ACS.

.5 Standard of Acceptance:
   - Kantech T-Rex
7.5. **Electronic Locks**

.1 Hardwired locks shall be electrified mortise, cylindrical, strike, rim and/or exit device. All locking devices shall meet the building, fire and electrical code requirements of all AHJ (authorities having jurisdiction).

.2 Unless otherwise directed by RPD, magnetic locks shall not be used.

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

.4 Electric locks shall fail-secure, unless otherwise directed by RPD.

.5 All electric strikes shall be 12/24VDC (unless AC is required for annunciation) and receive power from a dedicated power supply.

.6 Standard of Acceptance:

- Rutherford, Securitron, Folger Adam, HES
- Wireless lock solutions are not approved for use.

7.6. **Door Position Sensor**

.1 A door position sensor is required for all access-controlled doors.

.2 When door position sensors are used to monitor position for both the ACS and the IAS, sensors shall be minimum double-pole-single-throw (DPST) to provide single circuit operation, suitable for end-of-line supervision and connection to both systems.

7.7. **Remote Door Control**

.1 Certain doors may require the ability to be locked and unlocked remotely. This is to facilitate open/close, lunch hours, and security incidents where a quick method of locking the main door may be required, etc.

.2 A momentary switch may be used to provide control over these doors. The switch shall be integrated with the ACS to provide control, with status, and shall permit valid users to enter even when in the “locked” state.

.3 Status of the switch shall follow door state (i.e. lit when locked, unlit when unlocked).

.4 The relocking of doors, in the event they are accidently left unlocked, shall be protected by the following methods:

- Schedule to lock the door(s) at end of business hours.
- Integration with the IAS to lock the door(s) when the system is arming.

.5 Standard of Acceptance:

- Camden CM-30 Series (w/ red button and labelled “Push to Lock, Locked when Lit”)

7.8. **Remote Door Release**

.1 Certain doors may require the ability to be released remotely.

.2 A momentary push button switch may be used to provide control over these doors.

.3 The push button shall be integrated with the ACS for control of the door(s).

.4 The push button shall be clearly labeled as to which door is controlled.

.5 Standard of Acceptance:

- Camden CM-7000 Series (w/ black button and labelled, “Push to Open”)

- Honeywell IS310/320
8. VIDEO SURVEILLANCE SYSTEMS

8.1. General

.1 All instances of video surveillance for government use, require the approval of a Privacy Impact Assessment (PIA) as defined by the Office of the Information and Privacy Commissioner for B.C.

.2 Landlord owned video surveillance systems shall:
  .1 Not be located within, or with direct views of government tenant space;
  .2 Not utilize covert methods of video surveillance without government tenant consultation;
  .3 Must clearly identify purpose of video surveillance (e.g. theft prevention), landlord ownership and contact information, with appropriate signage, for any potential video surveillance related concerns from staff or members of the public, as per FIPPA legislation.

.3 The Video Surveillance System (VSS) shall not violate the rights of privacy and other legal rights of persons under observation. Signs shall be provided where routine surveillance is conducted, advising that the space is under electronic surveillance. Signage shall be in the languages spoken in the area. Cameras shall not be installed where there is a reasonable expectation of privacy; e.g. 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](http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/real-estate-space/video_surveillance_policy.pdf)

.4 All new video surveillance systems shall utilize an NVR (network video recorder) and IP (internet protocol) cameras.

.5 Required camera resolutions shall be identified in drawings as Story Board, Recognize or Identify as shown in Table 8.2.1.13.

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

.7 VSS shall be on a separate standalone network and shall not be connected to the government network without prior written approval from RPD.

.8 Cameras shall not be monitored at any off-site location without prior written approval from RPD.

.9 The VSS shall include all equipment necessary for a fully functioning system. It is the responsibility of the licensed security services provider to provision and maintain all security related devices including workstations, servers, networking hardware, etc.

.10 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 workstations.

.11 Cameras installed in highly sensitive areas shall provide full visibility (Identification) of person(s) entering the area. Cameras shall be mounted at suitable height for the required field of view and for clear unobstructed viewing.

.12 Cameras shall be monitored by an operator and/or recorded locally. Output shall be available for viewing by authorized persons.

.13 Where IP cameras are installed, wiring shall follow EIA/TIA 568/569 Standards.

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

.15 VSS (including all peripheral hardware) shall be protected from lightning and power surges.
8.2. **Surveillance Cameras**

.1 General

.1 It is the preference of RPD to utilize digital solutions. However, if an analog solution needs to be considered, consultation with RPD 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 shall be as discreet as possible. Color, finish and form factor shall be closely coordinated with the project architect to balance the use and function while maintaining the desired aesthetic.

.4 Cameras shall use a high resolution, progressive scan, 1/3” or greater CMOS imager with a varifocal/auto-iris lens and range capable of capturing the desired field of view.

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

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

.7 Exterior cameras shall be suitable for exterior installation environments and shall be provided with integral heaters, blowers, and seals necessary to operate within -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 for all exterior cameras.

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

.13 **Table: Scene/Resolution/Field-of-View**

<table>
<thead>
<tr>
<th>Scene Type</th>
<th>Resolution (pixels per foot)</th>
<th>Horizontal Resolution (pixels)</th>
<th>Vertical Resolution (pixels)</th>
<th>Maximum Horizontal Field of View (feet)</th>
<th>Maximum Vertical Field of View (feet)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Story Board</td>
<td>20</td>
<td>640</td>
<td>480</td>
<td>32</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>1024</td>
<td>768</td>
<td>51</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>1280</td>
<td>960</td>
<td>64</td>
<td>48</td>
</tr>
<tr>
<td>Recognize</td>
<td>40</td>
<td>640</td>
<td>480</td>
<td>16</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>1024</td>
<td>768</td>
<td>26</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>1280</td>
<td>960</td>
<td>32</td>
<td>24</td>
</tr>
<tr>
<td>Identify</td>
<td>80</td>
<td>640</td>
<td>480</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>1024</td>
<td>768</td>
<td>13</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>1280</td>
<td>960</td>
<td>16</td>
<td>12</td>
</tr>
</tbody>
</table>

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.
2. Analog Cameras:
   .1 Analog cameras are no longer accepted without consultation from RPD Security. Wherever possible, analog cameras shall be replaced with IP cameras and network cabling.

3. IP Cameras:
   .1 Cameras shall use H.264 (or newer) compression with a maximum 2 second key-frame interval.
   .2 All cameras shall be POE capable.
   .3 All cameras shall have the default login information changed. Information is to be documented and submitted as per this document.
   .4 All cameras shall be capable of being controlled and programmed through the VSS.
   .5 Standard of Acceptance:
      - IP Cameras: Axis, Avigilon, Bosch, Panasonic, Sony

8.3. Recording and Retention
   .1 New video surveillance systems shall utilize an NVR for recording video.
   .2 Cameras shall record at the maximum resolution available with a minimum per camera parameter of 1fps recording 24/7 and 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 manage all existing and new cameras (including Pan/Tilt/Zoom, pre and post recording of motion and analytic events, 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 enough capacity to accept all included cameras plus an additional twenty percent (20%) for potential expansion.
   .7 The VSS shall include all necessary licensed software (including operating system). It shall 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 The VSS shall be capable of extracting video in AVI format as well as the native file format with watermark. Native file format shall include an embedded player. Player shall not require installation or user privileges to play video.
   .10 The VSS shall 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 RPD. Contractor shall coordinate final mounting location at site prior to installation. Security equipment shall not share racks and/or cabinets with another client hardware.
   .12 Recording and network hardware shall utilize a UPS to provide a minimum of 30min backup power and filter AC. UPS shall 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 or generator where one is present.
   .13 UPS shall be connected to IAS as a 24hr supervisory alarm.
   .14 Video management software shall be fully programmed to provide suitable recording times (as per client requirements).
   .15 Standard of Acceptance:
8.4. **Video Surveillance Network**

.1 The network shall support an IP Surveillance System. This includes bandwidth, throughput, QoS, security, network services, and virtualization.

.2 The network shall be an isolated LAN that is not connected to the B.C. Government network, an ISP or any other 3rd Party network.

.3 Unless otherwise stated, the network shall not use any wireless technology. Wireless considerations require authorization through consultation with RPD Security.

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

.5 The network components shall 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 (CAT6) shall be terminated on RJ-45 data jack receptacles at each location and modular jack patch panels in equipment closets and main equipment rack cabinets. Provide CAT6 patch cords as required to connect cameras and interconnect switches at patch panels.

.8 Maximum length of CAT6 horizontal cable run shall not exceed 80 meters.

.9 Where CAT6 UTP cabling exceeds 80 meters, multimode fiber optic cabling shall be used instead with fiber to copper media converters.

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

.11 All installer passwords, switch configurations, serial numbers, IP and MAC addresses shall be documented and submitted as part of the project closeout documentation.

.12 Standard of Acceptance:

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

8.5. **Workstations**

.1 All workstations cabled directly to security systems, shall be located within a secure area (e.g. data room) and shall be managed either locally, or by:

- Associated keyboard, mouse and monitor functionality back to the operator location (KVM);

- Extension of the security LAN to operator location(s), and local small form factor workstation(s) with associated software clients. This solution requires consult and approval with RPD Security.

.2 All workstations shall use secure passwords for login and management.

.3 All workstations shall meet or exceed the minimum requirements specified by the VSS.

.4 All VSS workstation(s) shall include an LCD monitor, keyboard and mouse installed at designated operator locations.
8.6. **Monitors**

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

.2 Spot monitors shall be connected to digital video decoders for their associated streams.

.3 Monitors shall be wall or desk mounted unless otherwise specified.

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

.5 Monitors shall function normally without impact from local radio frequencies.
9. INTERCOM SYSTEMS

9.1. Audio Intercom

.1 The audio intercom station shall be installed on the exterior, next to the opening side of the designated entry door(s) at 1.4 m (54”) AFF. Master station(s) shall 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 integrated with the ACS so that they can remotely release the door. The contractor is responsible for all integration between these systems.

.3 Standard of Acceptance:
   • Aiphone IE Series

9.2. Video Intercom

.1 The video intercom station shall be installed on the exterior, next to the opening side of the designated entry door(s) at 1.4 m (54”) AFF. Master station(s) shall 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 integrated with the ACS so that they can remotely release the door. The contractor is responsible for all integration between these systems.

.3 Video intercom recording capabilities must not be enabled unless approved through a Privacy Impact Assessment (PIA).

.4 Standard of Acceptance:
   • Aiphone AX, JF, JK, JP and KB Series
10. PERIMETER INTRUSION DETECTION SYSTEMS

10.1. General

.1 Equipment for perimeter intrusion detection systems (PIDS) may consist of one or more of the following:
   .1 Fence Cut, Climb, Tamper Detection Systems
   .2 Electromagnetic Field Systems (microwave)
   .3 Video Surveillance Systems (VSS/PIDS Integration)
   .4 Video Surveillance Analytics
   .5 Perimeter Beam Systems
   .6 Ground Vibration (seismic) Systems
   .7 Other

.2 All perimeter intrusion detection systems require review by RPD Security prior to installation.

10.2. Fence Cut, Climb, Tamper Detection Systems

Fence cut, climb and tamper detection systems can be highly susceptible to false alarm and shall only be considered for controlled environments (e.g. maintained fence easement).

.1 The fence-mounted system shall detect vibrations from cut, climb or tamper 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:
   .1 Zones shall not exceed 15 linear meters (50 ft.) in length for optimum video surveillance assessment.
   .2 Zones shall not extend around corners in perimeter fencing.
   .3 Considerations for zoning shall include the reduction of nuisance alarms and assessment advantages for patrol personnel.

.3 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.

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

.5 All fence vibration detection zones to be on a separate partition. This partition shall be independent of all other alarm system partitions.

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

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

.8 Standard of Acceptance:
   • Southwest Microwave

10.3. Perimeter Beam Systems

Infrared beam systems are highly susceptible to false alarm and shall only be considered for controlled environments (e.g. alongside well maintained exterior fencing).

.1 Unless otherwise specified, beam towers to be configured so that the beams are set up in a “crossfire” pattern.

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

.3 All perimeter beam zones shall be on a separate partition. This partition shall be independent of all other alarm system partitions.

.4 Each perimeter beam to be an individual alarm zone (not ganged).
.5 Designated zones may be shunted as required by operational conditions.

.6 Beam towers shall be mounted and bolted directly onto contractor supplied 305mm (12”) diameter concrete pedestals (sunk minimum of 813mm - 32” into the ground).

.7 All cabling for the beam systems is to be installed in appropriately sized PVC electrical conduit (min. 20mm - 3/4”). All conduits to be buried to a minimum of 900 mm (36”). Installation shall meet code requirements of AHJ.

.8 All cabling to be of direct burial type and shall meet or exceed the manufacturer’s specifications.

.9 AC power for the perimeter beam system shall be a separate circuit and the circuit # shall be identified at the perimeter beam system control panel.

.10 Standard of Acceptance:
   - Optex Rednet series
   - Sicurit Absolute Pro Series
11. EXECUTION

11.1. Installation

.1 Whenever systems are being upgraded and/or installed, all abandoned cabling and devices shall 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 shall 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 because 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 RPD representatives and shall match the existing naming and classification schema.

.5 Contractor shall test and commission systems as fully operational and functional prior to handover. RPD reserves the right to verify the contractor’s test results to determine if system operation is satisfactory and contractor shall be responsible to correct any deficiencies for no additional cost.

.6 All cables shall be permanently identified and listed on as-built drawings as follows:
   .1 Cable number
   .2 Source
   .3 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.

11.2. 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 standards as required by the local AHJ (Authorities Having Jurisdiction).

.3 Contractor shall be responsible for insuring that all conductor types and gauges are enough 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 RPD.

.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 Wherever access control readers are installed, readers shall be cabled with 18/6 shielded cable (reader), 22/4 (tamper), and 18/2 TSP (Future OSDP).

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

.9 No splices shall be permitted in the wiring except when approved through consultation with RPD Security.
11.3. **Secure Termination**

.1 All security system control panels shall be in a secure, accessible location within the protected space (e.g., panels and equipment shall not be mounted in electrical or data rooms that are not within the protected space).

.2 All security systems shall 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.

11.4. **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 and soft conductor unless otherwise noted.

11.5. **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 comply with 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.

11.6. **Commissioning of Electronic Security Systems**

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

.2 The consultant or engineer to sign off that the system meets the full requirements of the system design and standards.

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

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

.5 Verification that all alarm signals have been received by the monitoring station.

**Paladin Technologies Monitoring Station**

1(800) 241-1122 or data@paladintechnologies.com
12. APPENDIX

12.1. Letter of Conformance

Project Name:

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

Section A:

<table>
<thead>
<tr>
<th>A.1</th>
<th>YES / NO</th>
<th>All security systems have been designed in compliance with the Physical Security Standards for Government of B.C. Facilities and any deviations have been identified, recorded and approved by RPD Security. Identify all deviations in Section B.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2</td>
<td>YES / NO</td>
<td>Complete intrusion alarm system (may include panic alarms) has been tested and all signals have been confirmed received by Paladin Technologies Monitoring Station.</td>
</tr>
<tr>
<td>A.3</td>
<td>YES / NO</td>
<td>Complete video surveillance system has been tested and all camera views have been verified and approved.</td>
</tr>
<tr>
<td>A.4</td>
<td>YES / NO</td>
<td>Complete access control system has been tested and functionality meets the requirements of the Physical Security Standards, contract documents and owners’ requirements.</td>
</tr>
<tr>
<td>A.5</td>
<td>YES / NO</td>
<td>Record drawings have been received, reviewed and are complete. Documents have all been submitted to: <a href="mailto:PhysicalSecurity@gov.bc.ca">PhysicalSecurity@gov.bc.ca</a></td>
</tr>
<tr>
<td>A.6</td>
<td>YES / NO</td>
<td>Training has been completed as per contract documents and owners’ requirements.</td>
</tr>
<tr>
<td>A.7</td>
<td>YES / NO</td>
<td>All security systems products and installation are in general conformance with contract document and shop drawings.</td>
</tr>
</tbody>
</table>

Section B: Deviations as per A.1 above (attach additional sheet if required)

<table>
<thead>
<tr>
<th>B1.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B2.</td>
<td></td>
</tr>
<tr>
<td>B3.</td>
<td></td>
</tr>
</tbody>
</table>

Person of Record:

Name: (print) Company:

Signature: Date:
### 12.2. OPR Checklist

<table>
<thead>
<tr>
<th>Item #</th>
<th>System</th>
<th>Commissioning and Acceptance Testing Standard</th>
<th>Submission</th>
<th>Initial</th>
<th>Date Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Design</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>The security system has been designed in compliance with the Physical Security Standards and all deviations have been recorded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Intrusion and Duress Systems</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>Verifications if all alarm signal communication to monitoring station and active account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Video Surveillance System</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>Video surveillance system functionality has been tested (including camera views) and meets the contract documents and client requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Access Control System</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>Access control system functionality has been tested and meets the contract documents and client requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Record Drawings</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>Record drawings and all other closeout documentation has been received, reviewed and are complete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>O&amp;M Manuals</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>O&amp;M manuals have been received, reviewed and are complete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Training</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>Training has been completed as per contract documents and client requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Security Installations</td>
<td>a. Physical Security Standards for Government of B.C. Facilities</td>
<td>All security systems products and installation are in general conformance with contract documents and shop drawings. This system installation conforms to the requirements of the Physical Security Standards.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### General Notes
a. If manufacturer has specific acceptance/commissioning testing requirements, they will be in addition to the standards listed above.