BRITISH COLUMBIA

REAL PROPERTY DIVISION

PHYSICAL SECURITY STANDARDS

for Government of BC Facilities

Date of Update	Author(s)	Revision Notes
06-22-2017	Chris Lien / Clayton Evoy (Ministry of Citizens' Services, Real Property Division)	Sections 1-11 (Full Revision)
03-01-2019	Chris Lien / Clayton Evoy (Ministry of Citizens' Services, Real Property Division)	Change Log 01032019 (available upon request)
04-24-2023	Chris Lien / Clayton Evoy / Eni Porbeni (Ministry of Citizens' Services, Real Property Division)	Significant Revision

Disclaimer

This document was prepared for the purposes of the Government 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 the information contained 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 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.

DEFINITIONS

The following definitions apply throughout this document:

- **ACS** – Access Control System
- **AHJ** – Authorities Having Jurisdiction
- **BUS/HSBS** – BC Government Building Utility Services network
- **CBRE** – RPD's Master Service Provider
- **DDRF** – Design Deviation Request Form
- **ESMS** – Enterprise Security Management System
- **IAS** – Intrusion Alarm System
- **IT Order** – internal government process used to order BC Government network connectivity from the OCIO.
- **OCIO** – Office of the Chief Information Officer
- **PIDS** – Perimeter Intrusion Detection System
- **RFI** – Request for Information
- **RPD** – Ministry of Citizens' Services, Real Property Division
- **VSS** – Video Surveillance System

1. APPLICATION

These standards apply to all space owned and leased by the Real Property Division, Ministry of Citizens' Services (RPD), and serve as minimum requirements.

New work must comply with this document. Renovation or reconfiguration of existing space requires the upgrading of the security system(s) to the requirements of this document.

Not all the systems or devices described in this standard shall necessarily be included in each project. It is the responsibility of the design team to consult and collaborate with the ministry client group to understand their operations, to build upon the Physical Security Standards, and develop a security design that meets the clients' functional requirements.

1.1 Purpose

The purpose of this standard is to ensure minimum requirements are established for security systems utilized within the BC Government. This documents the specific goals and objectives of RPD to define the major system software and hardware components that comprise the BC Government's Enterprise Security Management System (ESMS) and to provide design requirements for integration of the ESMS into new, existing buildings, and site development projects.

The principal goal of the document is to provide consistent design and implementation standards for physical and electronic security systems throughout BC Government facilities.

The ESMS is comprised of four major electronic security sub-systems:

- Intrusion Alarm System (IAS)
- Access Control System (ACS)
- Video Surveillance System (VSS)
- Perimeter Intrusion Detection Systems (PIDS)

Each of these sub-systems is comprised of command/control hardware, software, and field devices. The command/control hardware and software are standardized to provide the Government of BC with a unified operational platform for enterprise physical security management.

1.2 Design Deviation Request Form (DDRF)

All proposed deviations/exceptions to these standards require the submission of a DDRF. Do not assume that the deviation/exception is approved until the item has been specifically accepted by RPD. This form is included as Appendix 9.2.

1.3 Mandatory Systems – Minimum Requirements

An intrusion alarm system is a mandatory minimum requirement for securing any office, building or other BC Government space. Public facing locations shall also have a monitored duress alarm partition. Other systems within this standard are optional and require direction from the ministry client group(s) as to what is required for each location.

2. CONDITIONS

2.1 General

1. Items covered within this document shall not be cut and pasted as components of a consultant's specifications. It must be referenced as a complete document and not altered in any way.
2. Compliance with these standards does not imply a completely secure environment. Instead, these requirements shall be integrated into a comprehensive site security plan.
3. Security systems for government leased/owned space shall be managed solely by the BC Government. The use of landlord owned, and/or managed security systems is acceptable for common areas of buildings only and must not provide access to government leased space.
4. The BC Government shall have complete control of the operation of the system(s) while the space is occupied by the government and/or its tenants.
5. Equipment shall remain the sole property of the BC Government and the installing company shall not retain any ownership and/or control of the system(s).
6. Hardware, software, and operating systems required for operation, including programming, shall be provided. Hard copies of all required licenses/keys shall be provided.
7. Contractors shall take necessary measures to maintain security and prevent unauthorized access to government space, assets, and information during the performance of any work.
8. Security workstations, servers, controllers, and other devices shall be provided and maintained by a licensed security contractor and not by government entities (e.g., OCIO).
9. Remote access to security systems is not permitted. All considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).

2.2 Licensing

1. The consulting, design, engineering, and commissioning of electronic security systems for the Government of British Columbia shall be by qualified personnel that hold a Security Consultant license as per the British Columbia Security Services Act, regardless of any other professional designation (including P. Eng.).
2. Security contractors shall maintain current all licenses required to provide the specific work efforts of the project.
3. Security contractors shall utilize installation and service technicians holding a BC Security Worker License who are competent, factory trained, industry

certified, and capable of installing, maintaining the system(s), and providing reasonable service.

2.3 Design Requirements

It is the responsibility of the systems design team to identify (as part of the security drawings and specifications) the ministry client's functional requirements specific to each project, through documented communication with ministry client group representatives.

Security items shall be shown on dedicated drawings (Div. 28). The following items are required for review:

1. Specifications identifying the ministry clients desired systems and functional requirements specific to the project.
2. Floor plans, demolition plans, riser diagrams, and detail drawings
3. Project phasing plan (where applicable)
4. All end devices and controls (e.g., card readers, motion detectors, control panels, strobes, chimes, annunciators, duress switches, etc.) identified.
5. Intrusion alarm, access control, door, and video surveillance hardware schedules as applicable.
6. Relative Field-of-View (FOV) drawings for all video surveillance applications.
7. IAS and ACS partitioning

2.4 Material Substitutions

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 is intended to establish the type, function, standard of quality, and performance required. It is not the intent of RPD to exclude other materials, equipment, or processes.

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.

1. Consideration will be given to a proposed substitute when enough information is submitted to RPD through the Design Deviation Request Form (DDRF) to determine that the proposed material, equipment, or process is in fact equivalent (or better) in all respects to the materials, equipment, or process defined in these standards.
2. Substituted materials, equipment, or processes are not approved as equal until the item has been specifically accepted by RPD.

2.5 Training

1. Training shall be provided for two (2) hours per individual system (unless otherwise agreed) and be conducted at a time that is agreeable to both the security contractor and the ministry client.
2. The security contractor shall provide a list of individuals trained via an attendance sign-off sheet. This sheet shall identify the site, time, date of training, and items trained.

2.6 Warranty

The warranty period shall be a minimum of one (1) year parts and labor from the certified date of Substantial Performance of Work:

1. Defective equipment shall be repaired onsite and failing this, a suitable replacement unit shall be supplied (at no additional cost and within 24 hours) to keep the system fully operational until the original unit is returned.
2. Warranty certificate(s) shall include all company contact information including emergency after-hours support.

2.7 Handover/Closeout Documentation

The security contractor shall provide the following minimum documentation for each system:

1. User/Installation Manuals
2. Addendums and RFI's
3. As-built drawings (CAD and PDF) showing locations of all devices, controls, panels, keypads, strobes, sirens, and demarcation points. Zones and partitions shall be clearly identified in the drawings.
4. Monitoring company activity report verifying system testing.
5. All installer passwords, switch configurations, serial numbers, IP, and MAC addresses.
6. Warranty Certificate(s)
7. Completed Letter of Conformance (Appendix 9.1)
8. Any completed Design Deviation Request Forms (Appendix 9.2)

2.8 Reference Standards

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

1. CAN/ULC-S302-14 Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems
2. CAN/ULC-S316-14 Standard for Performance of Video Surveillance Systems
3. CAN/ULC-S318-96 Standard for Power Supplies for Burglar Alarm Systems

4. CAN/ULC-S319-05 Electronic Access Control Systems
5. CAN/ULC-437 Standard for Key Locks
6. ANSI/TIA-568/569 Standards for Commercial Building Cabling
7. British Columbia Building Code and Local Building Bylaws
8. Work Safe BC
9. All other applicable Federal, Provincial and Municipal laws, regulations, and bylaws.

2.9 Related Documents

1. British Columbia Security Services Act
2. RPD Technical Standards for Offices – Tenant Improvements
3. Privacy Guidelines – Freedom of Information and Protection of Privacy Act (FIPPA)
4. Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies
5. Privacy Management Accountability Policy (PMAP)
6. BC Government IMIT 6.11 Security Threat and Risk Assessment Standard
7. BC Government IMIT 6.24 Access Control Security Standard
8. BC Government IMIT 6.27 Operations Security Standard

3. EXECUTION

3.1 Work with Others - Cooperation

1. Coordinate and cooperate with other trades for timely completion of the work.
2. The security contractor shall coordinate work with RPD and their appointed representatives to ensure systems are installed, programmed, tested, commissioned, and verified fully operational to the satisfaction of RPD.

3.2 Installation

1. 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.
2. Whenever systems are being installed, or upgraded, all abandoned cabling and devices shall be removed.
3. Installation and service workmanship shall be accomplished in a neat and professional manner to meet best industry standards. The security contractor is responsible for the cleanup and disposal of all garbage and debris resulting from their work.
4. The security contractor shall repair at no cost to RPD any surfaces, finishes, equipment, or structures damaged by the execution of their contract, to the original condition.
5. 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 ministry clients and match existing naming and classification schema.
6. Security contractors shall test and commission systems as fully operational and functional prior to handover. RPD reserves the right to verify the security contractor's test results to determine if system operation is satisfactory. The security contractor is responsible for correcting any deficiencies at no additional cost.
7. Cables shall be permanently identified and listed on as-built drawings as follows: cable number / source / destination.
8. Where wiring penetrating any horizontal or vertical assembly is required to have a fire-resistance rating, the 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. Proposed exterior installations of security equipment require landlord acceptance prior to installation.

10. Security systems control panels, servers, storage arrays, etc. shall be wall mounted and/or installed within their own rack in the secure telecom room. Security equipment shall not share any rack with OCIO hardware.

3.3 Pathways

Wiring shall be concealed unless otherwise authorized by RPD:

1. Conduit shall be used when:
   a. Cabling is accessible to the public.
   b. Cabling may require mechanical protection.
2. Security cabling may be concealed within drop ceilings for:
   a. Staff areas
   b. Staff supervised areas (e.g., waiting room, program room)
3. Conduit connecting to field devices such as camera enclosures shall be terminated and secured up to the enclosure to conceal all wiring and connections.
4. When applicable, the security contractor shall coordinate installation of conduit and raceways with electrical contractor to meet these requirements.
5. Where ceiling pathways are utilized, cabling and installation shall comply with ANSI/TIA 568/569 Standards.

3.4 System Conductors & Cables

1. Provide cabling as required for all components as per manufacturers requirements.
2. The security contractor shall be responsible for ensuring that all conductor types and gauges are sufficient to meet requirements for power and control on all equipment being installed for use with the system. The security contractor shall provide any related calculations on request.
3. Network cabling shall be supplied, installed, terminated, and tested to fully meet ANSI/TIA 568 Transmission Performance Specifications. Test report shall be included with the O&M Manual.
4. Cables placed in underground ducts and conduit outside of buildings shall be rated for outdoor use with water blocking membranes.
5. Ground all security equipment as per manufacturer’s and AHJ requirements. Bonding conductor shall be green PVC jacketed, stranded copper and soft conductor unless otherwise noted.
6. Where fiber cable length is less than 300m, use a minimum of OM3.

3.5 Change Management

1. All changes to a system’s configuration shall be logged and associated with the individual making the 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.
3. Any other systems/processes that may be dependent on the system shall be identified and communicated to RPD.
4. A recovery plan shall be in place to restore the system should things not go as planned.
5. Post change testing is required to ensure the changed system, and any dependent systems, function as intended.

3.6 Commissioning

1. The consultant/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/engineer signs off that the system meets the full requirements of the design and standards by submitting a completed Letter of Conformance (Appendix 9.1).
3. On-site commissioning and provision of all personnel and equipment necessary to perform these tests shall be inclusive of each project referencing work included in this standard.
4. Commissioning shall include operational verification and testing of all new and existing devices installed, modified, or associated with the scope of the project.
5. Commissioning shall include verification that all alarm signals have been received by the monitoring station.

4. GENERAL REQUIREMENTS

4.1 Operational

1. Electronic security systems shall operate 24 hours a day, 7 days a week.
2. Daylight Savings Time (DST) shall be enabled.

4.2 Products

1. 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 Canadian Standards Association (CSA) or recognized approved equivalent.
3. All materials, including the hardware and software being supplied, shall be new and of the latest version or production model unless otherwise specified.
4. Foreign state-owned company products are not permitted.

4.3 Power

1. Security equipment shall be hard-wired to dedicated non-switched electrical circuits. The circuit numbers 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 (e.g., non-padlock-able “lock dogs”).
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 batteries and/or uninterruptable power supply (UPS) to provide a minimum of thirty minutes (30min) backup power to all security devices, when not protected by a generator. When protected by a generator, backup power shall be supplied until the generator comes online.
5. UPS equipment shall be integrated to signal the attached equipment to shut down properly in the event of a power failure.
6. Control panels shall have labels attached to their inside front covers indicating the equipment, electrical circuit, and date the battery was installed or last maintained.
7. All security systems shall be designed/installed with surge and lightning protection.

4.4 Passwords

All passwords for ESMS systems shall comply with the BC Government Complex Password requirements:

- Contain a minimum of ten characters.
- Contain characters from three of the following categories:
  - English upper-case characters (A to Z)
  - English lower-case characters (a to z)
  - Numerals (0 to 9)
  - Non-alphanumeric keyboard symbols (e.g., ! $ # %); and,
- Not contain the username or any proper names of the employees.

4.5 Network Connectivity

1. Intrusion alarm systems require a connection to the BC Government Building Utility Services network (BUS/HSBS). No other external network connectivity shall exist.
2. BUS/HSBS connectivity requires an IT Order created by the ministry client group.
3. Contractor shall contact OCIO Network Implementation (either via email OCIONetworkImpl@gov.bc.ca or telephone 250-387-5900 / 1-888-243-3222) to schedule an installation appointment. At time of appointment, technician shall be onsite and call into OCIO Network Implementation to provide MAC address of connected device and confirm connectivity.

4.6 Backups

1. Administration of systems shall include backups conducted per BC Government requirements. See IMIT 3.27 Operations Security Standard for more information.
2. System back-up procedures shall be part of initial systems training.

4.7 Telecom Rooms

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

1. Each telecom room requires:
   a. Entry doors equipped with door position sensors.
   b. A minimum of one (1) motion detector. Additional motion detectors may be required as determined by space.
   c. Intrusion alarm keypad (if required to be on its own partition)

d. Door closers for all doors that directly access the room. No door hold devices shall be installed or utilized.

e. Telecom rooms shall not be identifiable (including signage/graphics)

4.8 Door Hardware

1. Locks
   a. Grade 1 hardware is required.
2. Security Astragals
   a. Exterior doors require full-length astragals (to protect locking mechanism and deter against prying).
   b. Suite entry/exit doors and other interior doors that separate secure staff and client space, shall utilize form fitting astragals (to protect the locking mechanism only).
3. NRP (non-removeable pin) Hinges
   a. NRP hinges are required when exposed, for all exterior, suite entry/exit, and other doors that separate secure staff space from client space.

4.9 Key Control

1. Whenever possible, a complete keying protocol should be organized for the facility (e.g., perimeter doors locks should be keyed separately from other locks).
2. Keys, and any information needed to reproduce keys, should not be stored together. Master keys should remain in the building. Higher security areas/rooms should require dedicated keys.
3. Keyways shall use a “restricted” format at minimum and be engraved with “Do Not Copy”.
4. Where a higher level of security is required, keying shall be compliant with UL437 and be registered.

4.10 Physical Hardening

For locations that require a higher level of security, the following may be considered:

1. Doors
   a. Heavy duty 16 ga. solid core steel door (with steel stiffeners). Perimeter doors shall be fitted with a full-length steel astragal.
   b. Door and sidelight glazing may include heavy duty laminated glass or “attached” security window films installed to manufacturers specifications.

2. Windows
    a. Accessible windows (e.g., within 3 meters (10ft) of grade), may be protected with laminated glass or "attached" security window films installed to manufacturers' specifications.
3. Walls, Roofs, and Floors
    a. Interior demising walls shall be full height (slab to slab/roof) as required by technical standards. To increase the level of security, the following options may be considered:
        1. Walls, roofs, and floors may be constructed with 3.5mm (10 ga.) expanded metal mesh as a secure material layer where required.
        2. Construct the wall with a material designed to resist penetration (e.g.,13mm (1/2") plywood or particle board) as a backing to the outer layer of gypsum board wall finish.
        3. Construct the wall in the following order (from the exterior inwards):
            a. 16mm (5/8") gypsum wall board (or as per AHJ requirements)
            b. 3.5mm (10 ga.) expanded metal mesh
            c. 19mm Plywood or OSB
            d. Framing
            e. 16mm (5/8") gypsum wall board
            f. Where openings cannot be avoided at the ceiling plenum area, the area shall be completely enclosed with 3.5mm (10 ga.) expanded metal mesh.

4.11 Systems Hardening

1. Controller, expander, power supply and other security systems related enclosures shall be serviceable and have tamper-protection monitored as a supervised zone on the intrusion panel.
2. Systems shall be set up 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.
3. Access to systems shall be controlled and restricted to authorized personnel only. An approval process is required for access to be given, changed, or removed as per IMIT 6.24 Access Control Security Standard.
4. Services, applications, and user accounts that are not being utilized shall be disabled or uninstalled.
5. 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.

6. Methods shall be taken to disable the network, USB, and other ports that are not being utilized.
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. Security devices shall have the default user/password changed. The changed user/password shall be documented and submitted as per this document. Passwords should be unique to each device and compliant with Chapter 4.4.

5. INTRUSION ALARM SYSTEMS (IAS)

5.1 General

1. A monitored intrusion alarm system (IAS) is a mandatory minimum requirement for securing any office, building or other BC Government space. The IAS is designed to detect unauthorized entry into protected spaces. Locations that provide services directly to the public shall also have a monitored duress alarm that complies 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. 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.
4. The IAS may be divided into separate partitions (areas) as required.
5. Once the system installation is deemed substantially completed, the security contractor shall not access the system either physically or electronically without RPD consultation and written permission.
6. Intrusion protection shall be provided by way of hardwired door and window position sensors, with dual technology motion detectors (Note: glass break detectors shall only be used as an additional layer to motion detection for high security areas).
7. Each partition of the IAS shall have at minimum, the following devices:
    - Keypad
    - Door/Window Position Sensors (all entry/exit points)
    - Motion Detectors (covering all accessible perimeter windows, entry/exit doors, and main pathways)
    - Interior Siren
8. Control panels shall have labels attached to their inside front covers indicating the applicable zone descriptors.
9. Devices shall be supervised with End-of-Line Resistance (EOLR). EOLR shall be installed at the end device, not within the panel.
10. If used, terminal strips shall be mounted securely within an approved enclosure.
11. Upon completion of programming, the installer shall initiate an upload of the panel programming to the monitoring station.

12. Confirmation of all alarm signals received, with a report detailing the system's programming and configuration, shall be provided by the security contractor as part of the project document submittals.
13. Once the system installation is deemed substantially completed, the security contractor shall not access the system either physically or electronically without RPD consultation and written permission.
14. Standard of Acceptance:
    - DSC Maxsys
    - Bosch B and G Series
    - "No Equal"

5.2 Auto-Arming and Cancellation

1. Intrusion alarms shall auto-arm at multiple times (minimum 4) during evenings and weekends. The auto-arming schedules shall be performed by the IAS.
2. Recommended auto-arming times are 6pm, 8pm, 10pm, 12am (M-F) and 10am, 2pm, 6pm, 9pm (S-S).
    a. Consult ministry client 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.
    b. The annunciation and cancellation methods 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 warning shall be provided for three (3) minutes whenever the system is arming, whether manually or automatically. The warning tone shall be different from an alarm siren sound (siren pulse is not permitted) and shall be heard (minimum 10dB above average ambient sound level) throughout the protected space. The security contractor shall supply any additional sound devices if the space requires them to meet this stated criterion.
5. Notification requirements include offices and/or rooms with doors that can be closed. Ensure notification (dB) levels are compliant within these spaces.
6. A method of canceling 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.
    a. Momentary switches shall only provide cancellation during arming delay and shall not be capable of disarming alarm once armed.

7. Annunciators and cancellation devices shall be located within logical proximity to one another to facilitate ease of use.
8. Standard of acceptance:
   - Momentary Switch: Camden CM-7000 Series (w/ green button and labelled, "hold for 2 seconds to cancel auto-arm")
   - Annunciator: Flush Mount Single Gang 3 Tone Chime – W Box Technologies

5.3 Duress Alarms

1. Public facing offices shall have a monitored duress alarm.
2. Duress alarms shall not be installed within unsupervised areas accessible to members of the public.
3. Alarms shall be activated by hardwired devices only. Wireless duress alarm considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).
4. Devices located on movable furniture shall be connected using an RJ12 wall jack and a telephone patch cord to the jack.
5. Devices (and any associated wall jacks) shall be clearly identified by a machine printed label or other professional method.
6. Duress alarms shall be connected to a dedicated, monitored partition of the intrusion alarm and be programmed as a "24 Hour Duress" alarm.
7. When the alarm is activated, a flashing blue light and chime shall sound in designated staff areas. Signals shall not be heard/seen from duress initiating location to mitigate the potential for escalation.
8. In larger offices (where direct line of sight does not exist) and in higher security environments, duress alarms shall be shown on appropriately sized graphic annunciators) to simultaneously display all activated alarms.
9. Duress partitions require a dedicated keypad for the display and resetting of alarms.
10. Standard of Acceptance:
    - Audible Annunciator: 3 Tone Chime – W Box Technologies
    - Duress Devices: Magnasphere MK-3045 (under counter / wall mount applications)

5.4 Programming

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

2. The ministry client shall supply the security contractor with all user codes to be programmed into the alarm system.
3. The panel shall be programmed in SIA or CID format.
4. The security contractor shall program the following:
   a. Multiple monitoring stations receiver addresses for redundancy.
   b. User code required to bypass zones (no forced bypass). Auto-arming may use a code with forced bypass privilege.
   c. Daily test transmission (after 00:01 – 5:00, but not on the hour)
   d. Bell time-out shall be set at 4 minutes. Notification strobe to latch until reset.
   e. Automatic arming: multiple attempts (at least 4) throughout the unoccupied times (see Chapter 5.2).
   f. Automatic disarming is not permitted under any circumstance.
   g. Remote download access enabled.
   h. Intrusion panel upload code shall be changed from default and provided to the monitoring station.
   i. Installer code shall be changed from default and provided as part of the handover documentation.
   j. The security contractor shall not enable an installer's lockout.

5.5 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. Grade level or accessible windows that provide a large enough opening for a person, shall be equipped with a window position sensor.
3. Door position sensors shall be installed on the top, opening side of the door. Sensors shall be capable of initiating an alarm signal when the protected door is opened a maximum of 1" on the latch side.
4. Door and window sensors shall be "wide gap" type to align with false alarm reduction strategies.
5. Door and window sensors shall be a minimum of 3/8" diameter. Sensors shall be recessed unless otherwise required. 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. Exposed cabling shall be protected.
7. Overhead door sensors shall:
   a. Have aluminum housing and be equipped with an armored cable jacket.

   b. Be floor mounted with associated magnet surface mounted to the overhead door.

8. 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.

5.6 Motion Detectors

1. Motion detectors shall be used to provide internal area alarm detection covering all accessible perimeter windows, entry/exit doors, and main pathways.
2. Motion detectors shall utilize both microwave and passive infrared technology to reduce false alarms.
   a. Wall mounted motion detection preferred.
   b. 360° detectors may offer multiple modes of false alarm reduction versus dual technologies but must be suitable for the environment and application.
3. Motion detectors shall be installed, and field adjusted as per the manufacturer's specifications for appropriate coverage of the protected space.
4. Motion detectors shall have LED's disabled after initial testing is complete.

5.7 Glass Break Detectors

1. Glass break detection shall only be used as an additional layer to motion detection, for high security areas.
2. Glass break detectors shall provide low and high frequency detection to reduce the likelihood of false alarms.
3. Devices shall be installed, calibrated, and field adjusted as per manufacturer's specifications.

5.8 Keypads

1. No global operations permitted for keypads. Each partition shall have at least one (1) dedicated keypad.
2. Keypads shall be full alpha numeric.
3. Emergency buttons on an IAS keypad shall be disabled, unless otherwise directed by RPD.
4. Keypads shall have "Quick Arming" enabled. For example: (* then 0)
5. Keypads shall be installed fifty-four inches (54") above the finished floor. An additional keypad may be installed at an appropriate height for accessibility when required.

5.9 Sirens

1. A separate interior siren shall be installed within each partition.
2. An exterior siren may be installed where possible.
3. Sirens shall be programmed for a four-minute (4min) duration.

5.10 Alarm Notification Strobes

1. 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 activate until the alarm is reset by an authorized user.
2. The strobe shall be visible from the exterior of the secure space by arriving persons (e.g., viewable from window). An exception is made for sites that employ 24/7 security officers, providing for an immediate response.

5.11 Environmental Alarm Sensors

Where required, environmental alarm sensors may be installed and connected to the intrusion alarm system.

1. Environmental alarms shall be programmed as 24-hour zones and activated for continuous monitoring.
2. Environmental alarm sensors include:
   a. Low/High Temperature
   b. Water Detection
   c. Carbon Monoxide / Smoke Detection

5.12 Network Alarm Communicators

1. The security contractor shall provide a network alarm communicator connected to the IAS for reporting alarms over the BC Government Building Utility Services network (BUS/HSBS) as per Chapter 4.5.
2. Network alarm communicator connections to the BUS/HSBS require an IT Order completed by the ministry client group.
3. Communicator minimum specifications:
   - 128-bit AES encryption
   - Compatible with 10/100BaseT networks
   - Full duplex
   - Reports events to at least two (2) different receiver IP addresses

5.13 Cellular Backup

1. Cellular units shall be installed in locations where there is a moderate to strong cellular signal. If an acceptable signal level cannot be found within the premise, an exterior antenna solution may be required. Exterior locations require landlord approval.

2. 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.
3. The cellular unit shall monitor all signals from the intrusion system. These zones shall be identified as coming from the cellular communicator.
4. The cellular unit shall be capable of connection to the monitoring station.
5. Please see Chapter 5.14.5 for information on cellular SIM.

5.14 Monitoring

1. The Government of British Columbia retains the right to monitor alarm systems in a manner of their choosing and shall not be locked into any other monitoring arrangements because of alarm system installations.
2. Security contractor shall provide connectivity (hardware & software) with monitoring station:
    a. Typical Application:
        1. Primary network connection shall be through the BC Government Building Utility Services network (BUS/HSBS), with secondary cellular backup.
    b. High Security Application:
        1. Primary network connection through the BC Government Building Utility Services network (BUS/HSBS), secondary cellular backup, and tertiary telephone line backup.
3. 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”.
5. Monitoring is arranged by RPD’s Service Provider (CBRE), who will issue all relative information including receiver addresses and cellular radio SIM.

6. ACCESS CONTROL SYSTEMS (ACS)

6.1 General

1. Access Control Systems (ACS) may be installed when required by the ministry client. The system shall comply with the requirements of this document.
2. User information may contain business contact information (name, email, ministry, phone) only. The collection of photos or other personal information requires an accepted Privacy Impact Assessment (PIA) prior to implementation as per BC Government Privacy Management Accountability Policy (PMAP).
3. Card readers, electric locking devices, door position, 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).
4. The ACS shall include all new computer hardware, peripherals, and software necessary to operate the system as designed, including the recording of system event history. Materials shall meet or exceed the manufacturer's requirements.
5. The security contractor is responsible for providing and maintaining all security-related devices including workstations, servers, networking hardware, etc. for the ACS.
6. The ACS shall not be dependent on the workstation/server for its operation; 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.
7. The ACS shall have the number of cards immediately required by the tenant plus 20%.
8. For low security applications:
   a. The ACS may be integrated with the IAS to disarm when a valid access credential is presented. Systems shall continue to operate independently in the event of integration failure.
9. For medium to high security applications:
   a. The ACS shall not be integrated with the IAS to disarm when a valid access credential is presented. For these applications users shall enter with access card and then utilize a unique code on the intrusion keypad to disarm the alarm (multifactor authentication).
10. Whenever accessible door operators are installed on an access-controlled door, the door operator shall be integrated to activate only when the door is in the "unlocked state".
11. Communications between readers and controllers shall be OSDP (Open Supervised Device Protocol).

12. Standard of Acceptance:
    - Kantech EntraPass Corporate 8.6.1 (or higher)
    - Kantech Door Controller KT-400
    - “No Equal”

6.2 Scheduling

1. Scheduling shall not be used to control the state of doors except in the following circumstances:
    a. May be used to secure the door as part of the Remote Door Control solution identified within this standard.
    b. May be used for multi-tenant common building entrances, when in conjunction with “first-person-in” rules.
    c. May be used to control the state of a vestibule door (when other door is managed by Remote Door Control) and “first-person-in” rules are utilized.
2. All other door state scheduling considerations require RPD’s acceptance through the completion of a Design Deviation Request Form (DDRF).

6.3 Readers

The BC Government is migrating towards HID Seos as the preferred access control credential. As part of this transition path, the following requirements shall be implemented within each project:

1. New Systems:
    a. When a new system is installed, readers shall be HID Signo Seos profile, and a multi-technology credential may be used to bridge suite and base building systems.
2. Existing Systems:
    a. When an existing system requires a reader, the readers shall be HID Signo Seos multi-technology, capable of reading existing credentials.
3. Certain reader configuration changes may require authorization through HID Reader Manager Portal. All considerations require RPD’s acceptance through the completion of a Design Deviation Request Form (DDRF).
4. Bi-color LED shall provide the following minimum visual feedback: (RED = access denied, GREEN = access granted).
5. All readers shall be installed at an accessible height (36-48”) above the finished floor, unless otherwise directed. All wall-mounted readers shall be installed on a standard single-gang electrical backbox.
6. Exterior card readers shall be weatherproof, designed for outdoor applications, and installed on watertight boxes.

7. Readers shall be cabled according to manufacturer recommendations and for serial communications (OSDP) between controller and reader. All cables shall be sized appropriately for length and application.
8. Combination keypad/readers shall only be used for dual authentication (e.g., pin only not permitted).
9. Standard of Acceptance:
   a. HID Signo Seos:
      - Reader: 20TKS-T1-00C1W3 (mullion)
      - Reader: 40TKS- T1-00C1W3 (wall)
      - Keypad/Reader: 20KTKS- T1-00C1W3 (mullion)
      - Keypad/Reader: 40KTKS- T1-00C1W3 (wall)

   b. HID Seos/Prox (multi-technology):
      - Reader: 20TKS-00-00C1WC (mullion)
      - Reader: 40TKS-00-00C1WC (wall)
      - Keypad/Reader 20: 20KTKS-00-00C1WC (mullion)
      - Keypad/Reader 40: 40KTKS-00-00C1WC (wall)

   c. All other considerations require RPD’s acceptance through the completion of a Design Deviation Request Form (DDRF).

   d. “No Equal”

6.4 Credentials

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

1. New Systems:
   a. Whenever a new system is installed, credentials shall be HID Seos. A multi-technology card may be used to bridge suite and base building systems where possible.
2. Existing Systems:
   a. Whenever an existing system requires additional credentials, the existing credential type may be continued.
3. Credentials shall not have any identifying information (e.g., photo, address, ministry name, etc.) included or attached.
4. Standard of Acceptance:
   a. HID Credentials:
      - Seos Card: 5006PGGMN
      - Seos Key Fob: 5656PMSAV

- Seos/Prox Card: 5106RGGMNN

b. Credential Formatting:

- Corporate 1000 Format: H2006319
- Facility Code: 6370

c. Certain groups may utilize other Corporate 1000 formats (e.g., PSSG).

d. All other considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).

e. "No Equal"

6.5 Request-to-Exit (REX) Sensors

1. REX devices shall be configured to permit egress through monitored doors by shunting door position sensors upon activation. REX device shall not unlock door(s).
2. The REX shall have a built-in buzzer to locally annunciate "door forced" and "door held open" alarms.

6.6 Electronic Locks

1. 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. Locks shall be provided with appropriate wire transfer or electrified door hinge, which shall be cabled on the secure side of the door.
3. Electric locks shall fail-secure and be powered by 12/24VDC (unless AC is required for annunciation). Locks to be hard wired and receive power from a dedicated power supply.
4. Magnetic and wireless lock solutions are not approved for use. All considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).

6.7 Door Position Sensors

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.

6.8 Remote Door Control

Certain doors may require the ability to be locked and unlocked remotely (typically waiting rooms with client entrance doors). This is to facilitate open/close, lunch hours, and security incidents where a quick method of locking the main door may be required.

1. A momentary switch shall be used to provide control over these doors. The switch shall be integrated with the ACS to provide control, status, and permit authorized card holders to enter even when in the "locked" state.
2. The status of the momentary switch light indicator shall follow door state (i.e. lit when locked, unlit when unlocked).
3. The relocking of doors, in the event they are accidently left unlocked, shall be protected by the following methods:
   a. Schedule to lock the door(s) at end of business hours.
   b. Integration with the IAS to lock the door(s) when the system is arming.
4. Doors shall not automatically unlock by schedule or otherwise.
5. Standard of Acceptance:
   - Camden CM-30 Series (w/ red button and labelled "Push to Lock, Locked when Lit")

6.9 Remote Door Release

Certain doors may require the ability to be momentarily released remotely:

1. A momentary push button switch shall be used to provide control over these doors.
2. The push button shall be integrated with the ACS for control of the door(s).
3. The push button shall be clearly labeled as to which door is controlled.
4. Standard of Acceptance:
   - Camden CM-7000 Series (w/ red button and labelled faceplate, "Push to Open")

6.10 ACS Servers/Workstations

1. Servers and workstations shall meet or exceed the minimum requirements specified by the ACS.
2. Servers shall be cabled directly to the access control systems and be located within the secure telecom room.
3. Workstation(s) shall be located within the secure suite space as required for administration.
4. All ACS workstations shall include a monitor, keyboard, mouse, and latest version of software (including operating system and ACS application) supported by the ACS manufacturer.

7. VIDEO SURVEILLLANCE SYSTEMS (VSS)

All instances of video surveillance require an accepted Privacy Impact Assessment (PIA) prior to installation, as defined by the Office of the Information and Privacy Commissioner of BC and the BC Government Privacy Management Accountability Policy (PMAP).

7.1 General

1. Video Surveillance Systems (VSS) may be installed when required by the ministry client and supported by an accepted Privacy Impact Assessment. The system shall comply with the requirements of this document.
2. The 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, changing rooms, or other similar spaces.
3. Where a VSS is being provided, co-ordinate the equipment size and mounting with the electrical consultant to ensure proper sizing of the telecom room.
4. Required camera resolutions shall be identified in drawings as Story Board, Recognize or Identify as shown in Table 7.3.13.
5. Where the 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.
6. The VSS shall include all equipment necessary for a fully functioning system. The security contractor is responsible for providing and maintaining all security-related devices including workstations, servers, networking hardware, etc.
7. The VSS shall include all necessary licensed software (including operating system).
8. The VSS shall have the ability to switch frame rates on event without experiencing any loss in video recording.
9. The VSS shall have the ability to output to a DVD/R or USB drive and 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.
10. The security consultant/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, workstations, etc.

7.2 Video Surveillance Network

1. The VSS network shall be a dedicated, isolated LAN and not be connected to BC Government networks, an ISP, or any other 3rd party network.
2. The network components and performance shall meet or exceed the requirements specified by the VSS manufacturer.
3. The network shall support an IP Video Surveillance System. This includes bandwidth, throughput, QoS, security, network services, and virtualization.
4. 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.
5. The network shall be physically connected and not utilize any wireless technology. All wireless considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).
6. Data and other ports shall be disabled if not in use.
7. The VSS network shall utilize Cat 5e cabling at minimum, terminated on RJ-45 data jack receptacles at each location and modular jack patch panels in telecom room. Provide patch cords as required to connect cameras and interconnect switches at patch panels.
8. The maximum length of cable run shall not exceed 90 meters. Where cabling exceeds 90 meters, fiber optic cabling shall be used instead.
9. Security equipment shall not share any rack with OCIO hardware and may require its own floor or wall mounted rack/enclosures.

7.3 Cameras

1. Cameras shall utilize IP communications and be POE capable.
2. Cameras shall incorporate vandal/tamper resistant hardware. Level of resistance shall be appropriate for intended mounting location.
3. Color, finish, and form factor shall be coordinated with the project architect to balance the use and function while maintaining the desired aesthetic.
4. Interior cameras shall be suitable for interior installation environments.
5. Exterior cameras shall be suitable for exterior installation environments and provided with integral heaters, blowers, and seals necessary to operate within -40° to 50° Celsius (-40° to 122° F).
6. IR illumination shall be used as required to ensure that the area of interest is lit to the camera's requirements and is suitable for the scene type.
7. Cameras shall be mounted at suitable height for the required field of view and for clear unobstructed surveillance.
8. Cameras shall offer H.264 (or newer) compression.

9. Cameras shall have the default login information changed and passwords shall comply with Chapter 4.4 and be documented and submitted as per this document.
10. Cameras shall be capable of being controlled and programmed through VSS.
11. Under NO circumstances shall an empty housing or non-operational (dummy) camera be installed.
12. Resolution of cameras shall meet or exceed the minimum requirement for each type of scene as identified in the table below:

Storyboard: 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.

Scene Type	Resolution (pixels per foot)	Horizontal Resolution (pixels)	Vertical Resolutio n (pixels)	Maximum Horizontal Field of View (feet)	Maximum Vertical Field of View (feet)
Story Board	20 20 20	640 1024 1280	480 768 960	32 51 64	24 38 48
Recognize	40 40 40	640 1024 1280	480 768 960	16 26 32	12 19 24
Identify	80 80 80	640 1024 1280	480 768 960	8 13 16	6 10 12

13. Standard of Acceptance:
    - IP Cameras: Axis, Avigilon, Bosch, Panasonic, Sony

7.4 VSS Servers/Workstations

1. Servers/workstations shall meet or exceed the minimum requirements specified by the VSS manufacturer. All VSS workstations shall include a monitor, keyboard, mouse, and latest version of software (includes operating system and VSS application) supported by the manufacturer.
2. Servers shall be located within the secure telecom room.
3. Workstation(s) may be located within the secure suite space as required for administration.

7.5 Monitors

1. 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 may be wall or desk mounted. Mounting hardware to be provided as part of project.
4. Monitors shall function normally without impact from radio frequencies.

7.6 Recording and Retention

1. New video surveillance systems shall utilize a DVR/NVR for recording.
2. Cameras shall record at the required resolution for scene type, with a minimum 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. VSS shall be fully programmed to provide suitable recording times (as per ministry client requirements).
4. The VSS shall have the ability to record all images in a proprietary file format with forensic digital watermarking features.
5. 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.
6. The storage hardware shall be mounted in the secure telecom room. Security contractor shall coordinate final mounting location at site prior to installation. Security equipment shall not share any rack with OCIO hardware.

7.7 Landlord Owned Systems

Landlord owned video surveillance systems should comply with the following:

1. Not be located within or provide direct views of government tenant space.
2. Not utilize covert methods of video surveillance without government tenant consultation.
3. Clearly identify purpose of video surveillance, landlord ownership and contact information, with appropriate signage for any potential video surveillance related concerns from staff or members of the public, as per the Freedom of Information and Privacy Protection Act (FIPPA).

8. PERIMETER INTRUSION DETECTION SYSTEMS (PIDS)

8.1 General

1. Perimeter Intrusion Detection Systems (PIDS) may be installed when required by the ministry client. The system shall comply with the requirements of this document.
2. PIDS are highly susceptible to false alarm and should only be considered for controlled environments (e.g., maintained fence and easement).
3. The security consultant/contractor is responsible for ensuring the proposed solution is suitable for the environment where it is being installed (e.g., fence type/condition, controlled easement, existing vegetation management).
4. PIDS may consist of the following:
   - Fence Cut, Climb, Tamper Detection Systems
   - Perimeter Beam Systems
   - All other PIDS considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).

8.2 Fence Cut, Climb, Tamper Detection Systems

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:
   a. Zones shall not extend around corners in perimeter fencing.
   b. Considerations for zoning shall include the reduction of nuisance alarms and assessment advantages for patrol personnel.
3. The fence system shall:
   a. Detect climbing intruders with a weight of 34 kilograms (75 lbs.) with a Probability of Detection (Pd) of 95% at a 99% confidence level.
   b. Detect cuts to the fence fabric with a Probability of Detection (Pd) of 95% at a 99% confidence level.
   c. Be monitored by a dedicated partition of the intrusion alarm.
   d. Be on a dedicated AC circuit, with circuit # identified at the system control panel.
4. Fence vibration detection zones shall be monitored by a dedicated partition of the intrusion alarm.
5. Designated zones may be shunted as required by operational conditions.

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

8.3 Perimeter Beam Systems

1. Unless otherwise specified, beam towers shall be:
    a. Configured in a “crossfire” pattern.
    b. Equipped with thermostatically controlled heaters.
    c. An individual alarm zone (not ganged). Designated zones may be shunted as required by operational conditions.
    d. Mounted and bolted directly onto security contractor supplied 305mm (12”) diameter concrete pedestals (sunk minimum of 813mm - 32” into the ground).
    e. On a dedicated AC circuit with circuit # identified at the system control panel.

9. APPENDIX

9.1 Letter of Conformance

Project Name:

Instructions: The Person of Record (e.g., security engineer, designer, consultant) shall complete and sign this document. For each relative section, circle the corresponding answer below to confirm general compliance for the project. Person of Record shall complete and sign this document indicating conformance.

Section A:

A.1	YES / NO	Security systems are compliant with the Physical Security Standards for BC Government Facilities and any deviations/exceptions have been identified, recorded, and accepted by RPD. Identify all deviations/exceptions in Section B.
A.2	YES / NO	Complete intrusion alarm system (including any duress alarms) has been tested and all signals have been received by the monitoring station.
A.3	YES / NO	Complete video surveillance system has been tested and all camera views have been verified and approved by ministry client group.
A.4	YES / NO	Complete access control system has been tested and functionality meets the requirements of the Physical Security Standards, contract documents, and the ministry client group.
A.5	YES / NO	Record drawings have been received, reviewed and are complete. Documents have all been submitted to RPD.
A.6	YES / NO	Training has been provided as per contract documents and ministry client's requirements.
A.7	YES / NO	Security systems products and installation are in conformance with contract document and shop drawings.

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

B1.
B2.
B3.

Person of Record:

Name: (print) Company:

Signature: Date:

9.2 Design Deviation Request Form (DDRF)

Do not assume that the deviation/exception is approved until the item has been specifically accepted by RPD.

RPD Technical Standards

Design Deviation Request Form

BRITISH COLUMBIA

REAL PROPERTY DIVISION

It is RPD's expectation that when projects are being designed and implemented, the relevant technical standards shall be followed. However, it is understood that on some projects there may be justifiable reasons to deviate from a standard (e.g.: site constraints, landlord building standards, client requirements, etc.).

Under such circumstances and in conjunction with the Project Charter, the Design Deviation Request Form (DDRF) must be completed by the consulting team and submitted by the Prime Consultant to the RPD's Oversight Project Officer (OPO) or Development Manager (DM) assigned to the project. Submit a separate DDRF for each deviation request.

Upon receipt, the completed DDRF will be reviewed by RPD for acceptance, and signed off by the RPD OPO or DM.

It is RPD's expectation that any design deviations would be identified during the project schematic design phase however, it is understood that there may be exceptions (primarily security items) that may require deviations during other phases including construction.

Project Number:

Date:

*DDRF Number:

Project Name:

Project Address:

Deviation Subject Title:

Disciplines Affected: (*check off all applicable*):

__ Architectural __ Mechanical __ Electrical __ Security

Reference Clause Number(s) from Technical Standard: (*list all clauses affected and version of Technical Standard used)*)

Deviation Description: (*include any proposed options and supporting documentation*)

Rationale for Deviation:

Schedule Impact:	
Budget Impact:	
Applicant Name and Company:	Applicant Signature: Date Signed:

** The DDRF Number nomenclature shall comprise of the project number, followed by the discipline initial (e.g., Architectural = A, Mechanical = M, Electrical = E, Security = S, etc.), followed by the sequential number (e.g., 01, 02, 03).*

Review Comments: (*include BTA technical review comments and Consultant responses)*

Deviation Approval (RPD Use only):

__ APPROVED __ NOT APPROVED

RPD Oversight Project Officer / Development Manager Name:

Justification:

Date:

The completed form shall be attached to the Project Charter and added to the WDS Project Folder