Security Technology Standards

Version 1.30 – September 25th 2025

Vancouver CoastalHealth

Acknowledgement & References

This document contains information and ideas from many sources. We have gathered and used the experiences and ideas of others. We have adapted and applied them to the safety and security needs/requirements for VCH. Thank-you to those listed and not listed in this document for their advice and experiences that allow us to support a safe and secure environment of care for everyone.

Disclaimer

This document was created for use by Vancouver Coastal Health and is not intended to be used for any other purposes.

Security systems standards are constantly evolving. As a result, this document may be updated periodically without notice and may not accurately reflect the current Electronic Security Systems Standards within Vancouver Coastal Health.

Any reference to a product or service contained in this document does not constitute an endorsement or recommendation of that product or service by Vancouver Coastal Health.

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. This document and the information contained within may not be suitable for your purposes; any person relying upon any information in this document does so at their own risk.

Contents

VCH Protection Services (VPS)

Please contact your VCH Protection Services Representative or VCHProtectionSystems@vch.ca if you have any questions or need assistance with the content and use of this document.

Revision Log

Version	Who	Date	Detail
1.0	RDS	June 2024	New; Extracted from IPS ESSS 2024 & refreshed
1.1	RDS	Sept 2024	VCH Systems Email update
1.11	RDS	May 2025	Remove draft – Minor non technical updates
1.2	RDS	May 2025	- Addition - Glossary of Terms - Addition - Overdose Technology (ODT) (Sec 2.5) - Addition – Security Operations Centre (SOC) (Sec 2.1) - Update - Related Document Section (Sec 1.3) - Change – Document name - Clean up - section titles and formatting
1.21	RDS	12June2025	- Minor update - Overdose Technology (ODT) (Sec 2.5) - Approved Security Integrators (Sec 1.20)
1.22	RDS	10July2025	- Minor update - Overdose Technology (ODT) (Sec 2.5)
1.30	RDS/Team	15Sept2025	- Section 1 refreshed - Section 3 apendicies removed

1.0 GENERAL REQUIREMENTS

1.1 Overview Documents

1. This document outlines Security Technology requirements for all hospitals and/or healthcare facilities with in Vancouver Coastal Health (VCH).

    - This document is primarily intended for use at hospitals and/or larger facilities; however, the Protection Services department over sees electronic security systems/technology within VCH and is the designated representative for related matters.

2. The VCH Protection Services Department (VPS) oversees VCH Security Design Standards within Vancouver Coastal Health and is the designated authority for all security related matters. Any exceptions to stated requirements, including determination of approved equivalent products, must be approved in writing by a representative of VPS.

3. This document outlines Vancouver Coastal Health's Security Design Standards for the following:

    - Access Control Systems (ACS)
    - Duress / Panic Alarm Systems
    - Intercom Systems
    - Intrusion Detection Systems (IDS)
    - Overdose Detection Technologies (ODT)
    - Video Surveillance Systems (VSS)
    - Weapons Detection Systems
    - Other systems that may be used in the security, safety and security of people/property.

    NOTE: Some other systems (e.g. asset/infant protection, patient wandering) may integrate with the above noted systems. Where integration is appropriate, input on system design shall be required with clinical users/designate and VPS to ensure required functionality is achieved.

4. This document contains three sections. Consultants, contractors and others should refer to all sections to determine the full scope:

    - Section 1 - General Requirements: outlines requirements applicable work at all locations, generic system requirements, Security Integrators, etc.
    - Section 2 – Electronic Security Systems: outlines systems specific information including: Access control; CCTV; Intrusion alarm; Panic/Duress, Intercom.

5. Systems standards are constantly evolving and being updated. Sites in transition may require additional consultation. Contact VPS for any additional information required.

1.2 Related Documents

- Fraser Health - Security Design Standards v3 (2022)
- Guide for Using Overt Video Surveillance
- Interior Health - Integrated Protection Services Handbook
- International Association of Healthcare Security and Safety Basic (IAHSS) Industry Guidelines - http://www.iahss.org
- IPAC Canada
- IPS-Bike-Facility-Design-Guideline-Dec-2023-3.pdf (bcgreencare.ca)
- Owner's Project Requirements (OPR) for facilities | Vancouver Coastal Health (vch.ca)
- PHSA Communications & Infrastructure Standards & Specifications
- Physical Security Design Guidelines and Standards Version 1 October 2016 (alberta.ca)
- Physical Security Standards for Government of BC Facilities
- Privacy Guidelines – Freedom of Information and Protection of Privacy Act (FOIPP).
- Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies.
- Product Certification & Standards Development - CSA Group
- Security Services Act (gov.bc.ca)

1.3 Reference Standards

1. All materials, workmanship and/or installation practices and activity shall meet or exceed the following reference standards:
    - Canadian Electrical Code (CEC) Part 1 C22.1-00. BC Amendments to the CEC & associated bulletins.
    - BC Electrical Safety Act.
    - British Columbia Building Code.
    - British Columbia Fire Code Regulation.
    - TIA/EIA 568-B.1 through B.3 Commercial Building Telecommunications Cabling Standards.
    - TIA/EIA 569- B Commercial Building Standard for Telecommunications Pathways and Spaces.
    - ANSIA/TIA/EIA - 607A (J-STD-607-A-2002) Commercial Building Grounding and Bonding.
    - NEMA – National Electrical Manufacturers Association
    - Work Safe BC, Workers Compensation requirements.
    - Applicable Federal, Provincial and Municipal laws, regulations and bylaws.

1.4 Standard Requirements

1. Security Integrator(s) field staff and programmers shall be fully trained, and factory certified on all security systems utilized by VCH.
2. All Security Integrators and contractors are responsible for engaging the VPS Technology team directly, and in a timely manner, to ensure Security Technology design standards and operational expectations are met.
3. All equipment shall remain the sole property of VCH and the installing company shall not retain ownership or control of the system.
4. All hardware and software (including operating system) required to make programming changes to the systems shall be included with all systems. Hard copies of all software and/or licenses shall be provided if requested.
5. All systems shall be configured to be managed onsite; however, certain systems may require the ability to be remotely controlled and configured. The project scope and/or this document will identify those systems.
6. Panels, computers and other devices are not to be locked out (e.g. vendor supplied locking devices, electronically by password, etc.)
7. Provide all passwords to VPS, including installer, administrator, and the user passwords for all systems.
8. VCH maintains and manages a central “off-site/networked” Lenel access control head-end server and database for administration and programming of card access. All Lenel installations/additions at a facility must be networked to the Lenel Server by an VCH mandatory integrator. Refer to Approved Security Integrators Section 1.19.
9. Integrations between systems are often requested via project scope but 100% capability between systems is not achieved. The contractor is to report on any system(s) functionality that will not provide VCH with 100% integration prior to work commencing by the contractor.
10. VCH maintains and manages a central “on-prem storage” Video Surveillance System (VSS). Any new installations of a Video Surveillance system must integrate and be 100% compatible with the VCH Avigilon VSS.

1.5 Licences, Approvals, Permits & Standards

1. The VCH Protection Services (VPS) Department oversees Security Technologies within the VCH and is the designated representative for related matters. Any exceptions to stated requirements, including determination of approved equivalent products, must be approved in writing by a representative of VPS.
2. The Security Integrator shall be responsible for all building and electrical permits, licenses, inspections and related fees as required.
3. Prior to execution of work, the Security Integrator shall obtain all necessary permits and licenses for compliance with Federal, Provincial and Municipal laws and regulations.
4. On site Facilities Maintenance & Operations (FMO) and/or other health organization contacts are required to be consulted prior to the commencement of any work.
5. The Security Integrator and all workers must be provincially licensed and/or meet all requirements outlined as legislated in the BC Security Services Act.

1.6 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 conform to the standards of the Canadian Standards Association or CSA recognized approved equivalent. All materials, including hardware and software being supplied, shall be new and of the latest version or production model or match the existing version in use by VCH.
3. Equipment specifications are intended to provide a baseline reference for the type of materials that are to be installed. The Security Integrator shall ensure that all equipment being offered meets or exceeds the minimum requirements for intended operation.
4. Referenced manufacturers' products have been approved as standard equipment for installation within VCH facilities and shall not be substituted or replaced with non-approved alternates without written approval from the VPS representative.
5. Acceptable manufacturers required system components and owner supplied equipment may be site specific. If not detailed in the project scope, contact VPS for details and requirements.

1.7 Operational Requirements Including Response

1. Electronic security technology installed in VCH facilities shall operate on a 24-hour basis throughout the year.
2. All systems shall include sufficient back up power supply to operate all devices simultaneously without drawing more than 80% of the capacity of the power supply. The backup power system shall have sufficient capacity to operate the entire system for a minimum of 30 minutes under normal operating conditions.
   Note: All batteries to be minimum 7 (Ah) ampere hour.
3. Each system shall have sufficient power capacity 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 may require a local and/or regional response from the security service provider on site (where applicable). Methods for communicating system alarms and notifications vary from site to site and shall include the Security Operations Centre where required. Contact VPS to determine the required operational response communication method.

1.8 System Conductors and 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 camera installations to be IP/Networked based. Exceptions (e.g. analog cameras) require written VPS approval.
3. All IP/Networked cabling required for CCTV installations must follow the VCH/PHSA PHSA Communications & Infrastructure Standards & Specifications and installed by an authorized structured cabling vendor. Please contact PHSA for the most recent version of the PHSA Communications & Infrastructure Standards & Specifications.
4. All copper and fiber cable sheaths shall meet fire code requirements and comply with all applicable codes and meet all standards as required by the local AHJ (Authorities Having Jurisdiction).
5. Security Integrator(s) shall be responsible for ensuring that all conductor types and gauges required adequately power and control all equipment being installed for use with their system.
6. All wiring shall be concealed unless otherwise authorized, in writing, by VCH.
7. Cables placed in underground ducts and outside of buildings shall be rated for outdoor use with water blocking members.

8. In circumstances where analog cabling is required, Video Signal Cabling for analog devices for interconnection between equipment shall be minimum RG-59 type. For cable runs over 300 meters in length, RG-6 cable should be used. All CCTV coaxial cable connections shall be made using compression connectors only, twist on connectors are not permitted. Cat 6 and video baluns are acceptable. VPS to approve all analog installations if deemed necessary over IP.
9. No splices shall be permitted in the wiring except where a connection is made to a device. All connections shall be made using "B" connectors or approved equivalent. Ferrule terminations are required within the panels' where stranded cable is used. Marrettes and stakons connectors are not permitted.
10. All cables need to be labelled appropriately. Refer to Installation Section (Section 1.11) for cable labeling requirements.

1.9 Computers, Software and Software Related Licensing

1. Computers, servers, printers and other supporting peripheral equipment may be required as outlined in these specifications.
2. Hardware, computers, servers, printers and other supporting peripheral equipment, as required, can be provided by either by VCH (preferred) or via approved Security Integrator; to be determined on a case-by-case basis as approved by VPS.
3. The Security Integrator is required to ensure that all software versions provided are equivalent to the software currently in use by VCH.
4. Security Integrator supplied equipment to meet VCH requirements, where applicable.
5. Security Integrators are required to determine in advance, which equipment shall be supplied by VCH/PHSA, and which equipment shall be required to be supplied by the Security Integrator.
6. Where required, software/software licenses and any other required licensing is to be supplied by the installer/Security Integrator unless otherwise stated. This includes all software required for VCH's supplied hardware and equipment.
7. Door/reader and other licenses required for Lenel access systems shall be supplied by VCH for installations up to and including 32 doors.
8. Door/reader and other licenses required for Lenel access systems shall be supplied by the Security Integrator/installer for installations exceeding 32 doors.

NOTE: if Security integrator is not a Lenel VAR on record with VCH, a cash allowance (based on MSRP) for licencing must be carried. Refer to Approved Security Integrators Section 1.19 for contact and to obtain costs.

9. Lenel door licenses purchased by Security Integrators/installers to be a minimum of 64 readers.

1.10 Coordination of Work

1. Installations must be in accordance with manufacturers specifications, installation procedures, and fully comply with all applicable Codes and Regulations.
2. Coordination with PHSA may be required for computer, software and peripheral devices (including any wireless components).
3. Work may be required to be performed outside of regular business hours to avoid disruption to the delivery of patient care.
4. Installation Security Integrator(s) shall coordinate work with VCH and their appointed representatives to ensure systems are installed, programmed, tested, commissioning and verified fully operational to the satisfaction of VPS and VCH. VCH Reserves the right to verify the any test results to determine if the system operation is satisfactory. Contractor will be responsible for correcting any deficiencies at no additional cost to VCH.
5. Coordinate and cooperate with other trades, clinical staff, Infection & Prevention Control Practitioners and FMO, for timely completion of all work.

1.11 Installation

1. Installations shall be in accordance with the manufacturer's specifications and installation procedures and fully comply with all applicable Codes & Regulations.
2. Security Integrator shall test and commission fully operational and functional systems prior to turnover to VCH. VCH reserves the right to verify the Security Integrator’s test results to determine if system operation is satisfactory and Security Integrator shall be responsible to correct any deficiencies at no additional cost to VCH.
3. All cables shall be permanently identified using ¾” (minimum) printed nylon and/or vinyl labels and listed on as-built drawings as follows:
   a. On Cable Labels
      - Cable number
      - Device

b. On As-Built Drawings
   - Cable Number
   - Device
   - Source
   - Destination

4. Electrical panel circuit numbers shall be clearly identified on all system panels.
5. All work shall be installed in a neat and professional manner. The Security Integrator is responsible for clean-up and disposal of all garbage and debris caused as a result of their work.
6. Concrete cutting and/or coring may be required. In order to limit the disruption to patient care, cutting/coring may be required outside of regular business hours.
7. Wiring penetrating any horizontal or vertical assembly required to have a fire-resistance rating shall be in accordance with the local Authorities Having Jurisdiction (AHJ). Conduits or cables shall be tightly fitted and fire stopped where necessary to maintain fire rating.
8. Security Integrator(s) shall repair at no cost to VCH, any surfaces, finishes, equipment or structures damaged by the execution of their contract to its original condition.
9. All security system control panels shall be located in a secure, accessible location. Head-end security equipment for Access Control, CCTV, Intrusion/Panic alarms shall be mounted at locations designated by VPS. Deviation from this requires written consent from VPS.
10. Ground security equipment as per manufacturer's recommendations.
11. Bonding conductor shall be green PVC jacketed, stranded copper, soft conductor, unless otherwise noted.
12. All digital inputs are required to have end of line resistor(s) to achieve four state supervision.
13. VCH's security systems do not require conduit with the following exceptions: exposed or exterior locations or where required by other VCH departments and/or facility policy (FMO, PHSA).
14. All wiring shall be concealed unless otherwise authorized by VCH.
15. Wall mounted devices to be secured to wall studs and/or installed with plywood backing sufficient to support device weight.
16. Ceiling mounted devices to be secured with sufficient backing to support device weight and meet seismic requirements.
17. All wiring and cable installed and connected to any piece of security equipment that is accessible to the public shall be installed in conduit or protective

covering. Conduit connecting to field devices such as camera enclosure shall be terminated and secured up to the enclosure to conceal all wiring and connections. Where applicable, the Security Integrator shall coordinate installation of conduit and raceways with the electrical contractor to meet these requirements. Note: Conduit not to be filled past 40% capacity.

18. Due to public private partnership arrangements, service contracts and potential other factors, it may be mandatory for installation, programming or other work be completed by designated companies only. If applicable, this information shall be listed in the project scope and/or defined in this document.

1.12 Programming

1. Programming of all systems to be completed in full by the Security Integrator, in consultation with VCH Protection Services (VPS).
2. Programming of all system devices and components are to be done to the satisfaction of VPS.
3. All installations require system embedded floor plans/maps with device locations.
4. Access control database programming must be completed by VCH's designated Security Integrator. Refer to Approved Security Integrator Section 1.19).
5. The installation contractor is to cover all associated costs of programming. Note: Access Control and Video Surveillance systems programming must be completed by a mandatory integrator (Refer to Approved Security Integrator Section 1.19). If Contractor is not a VAR on Record with VCH, a cash allowance (based on MSRP) for this work must be carried.
6. VCH Protection Services will provide the naming convention(s) required for programming all protection technologies devices/zones/etc.
7. Due to public private partnership arrangements, service contracts and potential other factors, it may be mandatory for installation, programming or other work be completed by designated companies only. If applicable, this information shall be listed in the project scope and/or defined in this document.

1.13 Documentation

1. Security Integrator shall provide the following documentation to VCH PS:
   - All installation and user manuals are to be provided in electronic form.
   - Equipment schedule detailing installation.
   - Provide map overlay (as-buit) with locations of all devices, controls, demark connection, panels, keypads, risers diagrams, and panel termination details identified. Drawings to be provide electronically in a format suitable to VPS.
   - All zones shall be clearly identified on the as-built drawings.
   - Electrical panel circuit breaker shall be clearly identified and noted on both the panel cover and as-built drawings.
   - A printout of the monitoring company activity report that verifies full system testing in electronic form.
   - Device verification sign-off sheets, electronic and/or paper, if required.
   - Manufacturer's cut sheets for all devices, electronic and/or paper, as required.
   - Infection Control documentation, as required.
   - Documentation outlining the IP schemes utilized in the installation
   - All forms completed as supplied by VCH.
   - Municipal and other required electrical permits.
   - Warranty Certificate, as required.
2. All documentation to be submitted to VCH's designate, as required.
3. Security Integrator(s) shall provide VCH with a training attendance sign-off sheet. This sheet shall identify the site, time and date as well as a listing of all those in attendance, electronic and/or paper.

1.14 Training

1. Training shall be provided for each individual system as required by this document. Training shall include a minimum of four (4) hours per individual system, if required (to be determined by VPS), and shall be conducted at a time that is mutually agreeable to both the Security Integrator and VCH.

1.15 Warranty

1. The warranty period with respect to the Contract is minimum one (1) year from the certified date of Substantial Completion of Work.
2. Defective equipment to be repaired at site and failing this a suitable replacement unit shall be supplied to keep the system operational until the original unit is returned.

1.16 Alarm Monitoring

1. VCH may require off site ULC rated alarm monitoring service to facilitate a personnel response to system generated alarms.
2. All alarm systems and ancillary equipment shall conform to VCH Protection Design Standards.
3. VCH requires all alarms to report to the VCH Security Operations Centre via established alarm reporting pathways. Alarm reporting pathways to be determined in consultation with VPS. Also see Section 2.1 Security Operations Centre for guidance.
4. Account numbers and other applicable information shall be provided by Health Organization's authorized monitoring agent/station monitoring station.
5. Refer to Approved Security Integrator Section 1.19) for off-site monitoring company.
6. The Security Integrator is to cover all associated costs of programming and monitoring set-up, if required.

1.17 Security Integrator Responsibilities

1. All Electronic Security Systems and its related hardware and software are to be installed as per manufacturer specifications.
2. The Security Integrator shall ensure that all required information is provided and recorded on VCH's authorized monitoring agent/station as required.
3. The Security Integrator shall complete the user list in conjunction with the client (tenant) who shall provide details of appropriate users. Security Integrator shall fully program the system accordingly.
4. The Security Integrator is responsible for all associated costs of programming and monitoring set-up, if required.
5. Access to the system for post installation warranty/deficiency service, or other required access, to be coordinated with VPS.
6. All passwords for all devices to be supplied to VPS.

7. All information related to installations are considered strictly confidential and the Security Integrator shall guarantee non-disclosure of information unless otherwise authorized by VPS, in writing.

1.18 Client (Tenant) Responsibilities

1. Once the system is installed and commissioned, VCH's (tenant) is responsible to manage the Client User List function and maintain the database ensuring that all subsequent changes to personnel are noted and reported to VPS & VCH's authorized monitoring agent/station.
2. All Information is to always remain confidential.

1.19 Approved Security Integrators

1. Security Integrators are required to have the appropriate credentials and to be approved/in good standing with the security system's manufacturer to perform installation and/or service on VCH security systems/technology.
2. Preferred Security Integrators (alphabetically) for listed systems include:
   - Centre Electrical + Technology: www.cecgrp.ca
   - Convergint Technologies: https://www.convergint.com/
   - Houle Security: https://www.houle.ca/
   - Paladin Technologies: https://paladintechnologies.com/

3. Lenel OnGuard - Mandatory Security Integrators (alphabetically) required installation/programming and commissioning/verification of any Lenel access control and alarm monitoring devices, including integrations:
   - Paladin Technologies: https://paladintechnologies.com/

4. GuardRFID RTLS - Mandatory Security Integrators (alphabetically) required installation/programming and commissioning/verification of any GuardRFID devices, including integrations:
   - Paladin Technologies: https://paladintechnologies.com/

5. Sonitor RTLS - Mandatory Security Integrators (alphabetically) required installation/programming and commissioning/verification of any Sonitor devices, including integrations:
   - Houle Security: https://www.houle.ca/

6. Monitoring - Mandatory off-site alarm monitoring stations (alphabetically) required for offsite monitoring when required:
   - Paladin Technologies: https://paladintechnologies.com/

7. Overdose Detection Technologies - Mandatory Security Integrators (alphabetically) required installation/programming and commissioning/verification of any Overdose Detection Technologies, including integrations:
   - Centre Electrical + Technology: www.cecgrp.ca
   - Houle Security: https://www.houle.ca/
   - Paladin Technologies: https://paladintechnologies.com/

   NOTE: Due to public private partnership arrangements and associated service contracts, it may be mandatory for installation, programming or other work be completed by designated companies only. If applicable, this information shall be listed in the site specific information contained in the site appendices.

2.0 ELECTRONIC SECURITY SYSTEMS

2.1 Security Operations Centre (SOC)

2.1.1 General

1. As of April 1st 2025 VCH has opened a Security Operations Centre.
2. SOC Operations and standards in development
3. All security systems installations and alarm responses are to consider the Security Operations Centre and its operation.
4. Contact VPS for more information

2.2 Access Control Systems (ACS)

2.2.1 General

1. All hardware and software required for the system to operate are to be installed as per manufacturer's specifications.
2. Access control system shall be installed in protected space based on client requirements. Card readers and electric locking devices shall be installed at all designated entry doors to the protected space, including stairwell doors at points of public access.
3. Elevator control, where required, shall be installed to allow for control of the elevator on a floor by floor basis.
4. The Security Integrator shall provide new hardware and software/licensing for all installations. Existing spare capacity shall not be utilized unless approved, in writing, by VCH PS.
5. Every door equipped with a card reader and electric locking device shall also have a door contact to monitor held open/door forced open functions and request to exit (REX) sensor as required by the Health Organization.
6. Every door equipped with a card reader and electric locking device shall also have a mechanical key override to be used in the event of a system failure.
7. The access system shall not be dependent on the system workstation or server computer for operation required to operate basic card access functionality including card read, door lock/unlock. The system control panels and field hardware shall be able to continue to operate 24 hours a day, 7 days a week without any degradation in the operation of the system in the event of workstation, computer or server downtime/failure.

8. Magnetic locks are not permitted unless authorized in writing by the Health Organization.
9. Sliding doors are not acceptable on medication rooms or doors into any room, area or department that are deemed high security risk by VCH PS.
10. Card readers are to be proximity type.
11. Card readers may also be required to have PIN code authentication in addition to proximity authentication.
12. Where dual authentication is required (PIN code and Proximity) the PIN code feature is to be fully integrated in to the card reader with full functionality in the access system and software. Parallel, separately installed pin devices are not acceptable unless approved in writing VCH PS.
13. Access control database programming must be completed by the Health Organization's designated Security Integrator. Refer to Acceptable Security Integrator section.
14. Acceptable manufacturer, required system components and Health Organization's supplied equipment may be site specific and as outlined in the attached appendices.

2.2.2 Card Readers

1. Readers shall be connected to door controller via standard Wiegand interface.
2. Readers shall be HID Signo unless approved in writing by VCH PS.
3. Readers must be capable of reading HID Corporate 1000 card format.
4. Bi-color LED controlled locally and by host system shall provide at the minimum following visual feedback: (RED = door locked, GREEN = access granted).
5. Exterior card reader shall be weather proof, designed for outdoor applications in the applicable environment.
6. All readers to be installed at 1.2m (46") above finished floor unless directed otherwise by the Health Organization.
7. All wall-mounted readers shall be designed for installation on a standard single-gang electrical back-box.
8. Mullion sized readers may be used in locations with limited mounting space.
9. Readers shall be black unless otherwise specified.
10. Where there are multiple card readers in close proximity, integrated card reader locksets will be considered; style and manufacturer must be approved in writing by the Health Organization.

2.2.3 Request to Exit (REX) Devices

1. REX devices shall allow egress through monitored doors without creating alarms with REX connected to bypass door alarm on exit.
2. REX devices to meet required functionality.
3. REX motion devices shall have a built-in buzzer to locally annunciate "door forced" alarms and "door held open" warnings. Local buzzer to remain **OFF** unless requested to be turned on by VCH PS.
4. REX switches shall have a local buzzer to annunciate "door forced" alarms and "door held open" warnings. Local buzzer to remain **OFF** unless requested to be turned on by VCH PS.
5. Latch bolt monitors cannot be used as REX devices.
6. REX motion sensors shall have the following minimum features:
    - X-Y Targeting - targets a specific area of detection
    - Digital Signal Processing
    - Curtain type Fresnel lens
    - Detection range 3 to 6 meters
    - Main relay timer (adjustable delay .5 to 60 seconds)
    - Selectable relay trigger mode
    - Sounder volume to 90dB
    - Activation LED
    - Tamper switch

2.2.4 Electrified Hardware

1. Unless otherwise specified, electric strikes or integrated locksets are the only acceptable electric locking devices. All locking devices must meet the building, fire and electrical code requirements of all Authorities Having Jurisdiction (AHJ).
2. Unless otherwise directed electric strikes shall fail "secure"
3. Acceptable manufacturers: Dependent on site standard for locks and hardware.

2.2.5 Door Contacts

1. All door and window contacts must be "wide gap" type.
2. All door and window contacts must be concealed unless otherwise directed. If installed in wood or similar material, allow for expansion. Fill all voids with RTV silicone or equivalent.
3. Latch bolt monitors cannot be used as door contacts.

2.2.6 Remote Door Control

1. Where required, designated doors shall have a control switch(es) installed to control door lock and unlock functions.
2. Access control workstations shall not be utilized for remote door control unless authorized in writing by the Health Organization.
3. The switch shall be integrated with the access control / card access system where applicable.
4. The switch shall be illuminated to indicate and differentiate between all status functions
5. Switch functions to include permanent lock; permanent unlock; momentary unlock.
6. Acceptable manufacturers are site specific and outlined in the attached appendices.
7. Make and model of switch shall be approved by VCH PS.

2.2.7 Access Control System Programming

1. Access control head end/database programming must be completed by the designated Health Organization Security Integrator. Refer to List of Security Integrators. Pricing structure as per pre-determined rates established by VCH PS and the designated Security Integrators.
2. Readers must not remain programmed in Facility Code Only Mode (online or offline); card programming must be card, PIN, or card and PIN only.
3. Required programming includes, but not limited to, labeling/naming all devices, graphic user interface, and client software/user setup.
4. Electronic versions of floor plans, if required, to be supplied by the Health Organization.

2.2.8 Integration Requirements

1. Other security systems are not to be integrated into Access Control Systems with out the written consent of VCH PS.

2.3 Video Surveillance Systems (VSS)

2.3.1 General

1. All hardware and software required for the system to operate are to be installed as per manufacturer's specifications.
2. Vendor supplied appliances must be authorized by the Health Organization.

3. Network switch ports must be supplied by the Health Organization; vendor supplied appliance switch ports are not to be used unless approved by the Health Organization.
4. Cameras that are clinical or specialized in nature need to be approved by VCH PS before they can reside on the Security surveillance infrastructure.

2.3.2 CCTV Applications

1. CCTV systems can be utilized, but are not limited to, the following applications:
   - Site Security
   - General Clinical Observation
2. This specification is designed to outline the requirements related to the above stated uses. This specification is not designed for use with other/specialized applications (e.g. operating rooms, labour delivery rooms, treatments rooms, specialized clinical sleep laboratory).

2.3.3 Site Security CCTV Systems

1. Security CCTV systems shall not violate the rights of privacy and other legal rights of persons under observation. 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 "Public Sector Surveillance Guidelines":
   - https://www.oipc.bc.ca/resources/guidance-documents/
2. The CCTV system shall include all equipment necessary for a fully functioning system.
3. Cameras installed at entry and/or exit points and in elevated risk areas (e.g. pharmacy, maternity, etc.) shall provide full visibility of person(s) entering the area. Cameras must have the ability to identify the following, but not limited to: facial features, clothing and other identifiable details.
4. The CCTV system shall provide recorded images of sufficient quality to be used as court evidence in Canada.
5. Output must be available for viewing by authorized persons at multiple locations, if required.
6. Indoor/outdoor camera enclosures, where accessible by the public and/or within a 12' height, must be vandal resistant domes constructed of high impact polycarbonate material or approved equivalent.

7. Only IP cameras are acceptable for security CCTV systems. Megapixels to be determined by field of view. Installation is required to be in compliance with Health Organization cabling standards.
8. Plywood backing required for wall mount monitor installations to meet seismic requirements.
9. Exterior enclosures/equipment must be NEMA rated.
10. Cameras and enclosures used for clinical purposes or in clinical areas must be rated by the manufacturer for use in the specific environment (e.g. cameras for seclusion rooms must be anti-ligature and specifically designed for high risk clinical environments).
11. Required system components and Health Organization supplied equipment is site specific and outlined in the attached appendices.

2.3.4 General Clinical Observation CCTV Systems

1. Cameras within Clinical units shall have the ability to record. Health Organization to determine which camera(s) are recorded.
2. The CCTV systems shall include all equipment necessary for a fully functioning system.
3. Output must be available for viewing by authorized persons at multiple locations, if required.
4. Non-recorded Clinical camera systems are to be viewed by authorized clinical staff only. Camera system user accounts/permissions to be programmed by VCH PS.
5. Indoor/outdoor camera enclosures must be vandal resistant domes constructed of high impact polycarbonate material or approved equipment.
6. Coax cable installations are acceptable for Clinical CCTV systems. If an IP based solution is utilized, the installation is required to be in compliance with PHSA cabling standards.
7. Exterior enclosures/equipment must be NEMA rated.
8. Cameras and enclosures used for clinical purposes or in clinical areas must be rated by the manufacturer for use in the specific environment (e.g. cameras for seclusion rooms must be anti-ligature and specifically designed for high risk clinical environments).
9. Required system components and Health Organization supplied equipment is site specific and outlined in the attached appendices.

2.3.5 Elevated Risk Areas

1. Where controlled substances are stored outside of Pharmacy, regardless of whether the items are stored in a dispensing unit (Pyxis), cupboard,

drawer or other, CCTV surveillance to directly observe and record the storage location (min. 1 camera) is required for all installations.

2.3.6 Artificial Intelligence (AI) and Video Analytics

1. All cameras shall be capable of, but not limited to, the following Artificial Intelligence (AI) and Video Analytics: Appearance Search, Facial Recognition, Focus of Attention (FoA), and License Plate Recognition.

2.3.7 Cameras

1. Unless specified otherwise, all cameras shall be dome type. Indoor/outdoor camera enclosures with vandal resistant domes constructed of high impact polycarbonate material, plenum rated back box and UV resistant smoked optically clear acrylic lower dome with maximum of f/0.5 light loss and tamper resistant hardware. Diameter of lower dome shall be low profile, maximum 6".
2. The camera shall be high resolution color [minimum 4 megapixel (MP)] and must automatically switch the camera from color to black and white mode in low light conditions.
3. Cameras that are subject to extreme low light conditions must be equipped with infrared illuminators.
4. Camera resolution is to be selected to achieve a minimum of 60 pixels per foot on target. Approximate coverage is as follows based on a mounting height of 10':
    - 2.0 MP dome cameras with 3-9mm lens; greater than 1MP FOV up to 50' length x 30' wide (FOV)
    - 3.0 MP dome cameras with 3-9mm lens; greater than 2MP FOV up to 60' length x 35' wide (FOV)
    - 5.0 MP (minimum) dome cameras with 3-9mm lens; greater than 3MP FOV up to 80' length x 45' wide (FOV)
5. The outdoor camera shall offer protection against the elements. The camera's operating temperature range shall be -30° to 50° Celsius
6. All camera shall operate on POE, POE+ and POE++ require network switch compatibility.
7. Where IP cameras are installed; all cameras and converters shall integrate with site specific recording platform.
8. Non IP camera connections shall be crimped.
9. Acceptable recording platform manufacturers are site specific and outlined in the attached appendices. Cameras: Avigilon and Avigilon

compatible cameras (with full feature Avigilon integration). Any other manufacturer camera(s) must be approved by VCH PS.

2.3.8 Video Recording System and Storage

1. Video recording platforms and requirements may differ depending on location. Required system components and Health Organization supplied equipment is site specific and outlined in the attached appendices.
2. Devices shall include all necessary software (including an operating system) and have a time/date generator and emergency and alarm recording features.
3. Where Health Organization's storage shall be supplied, the Security Integrator/installer is required to provide storage calculation requirements to ensure adequate storage/additional storage is provided by the Health Organization.
4. Motion only recording is acceptable. Data retention/storage to be supplied for a minimum of 30 days and have minimum frame rate of 24 frames per second (FPS).
5. Data storage days to be calculated utilizing RAID 6 for acute sites, unless otherwise approved by VCH PS.
6. NVR's must have the ability to output to a USB removable media drive.
7. Devices to be mounted in a secure location as directed by the Health Organization. Security Integrator shall coordinate final mounting location at site prior to installation.
8. Devices to be fully programmed to provide suitable recording times (as per client requirements).
9. Acceptable manufacturers are site specific and outlined in the attached appendices.

2.3.9 Monitors

1. Monitors shall be wall, ceiling or desk mounted as per the Health Organizations' requirements.
2. All monitors shall be high resolution, TFT active matrix LCD monitor, with multimode functionality, minimum 1920 x 1080 resolution – minimum 24", unless otherwise approved by the Health organization.
3. Acceptable manufacturers are site specific and outlined in the attached appendices.

2.3.10 CCTV System Programming

1. Required programming includes, but is not limited to, labeling/naming all devices (as per Health Organization naming convention) and client software/user setup.
2. Where available in the CCTV system, device mapping is required unless otherwise stated by VCH PS.

2.3.11 Integration Requirements

1. Other security systems may be integrated into CCTV Systems. This will be determined on a case by case basis and written approval from VCH PS is required prior to any integration.

2.4 Intrusion Detection Systems (IDS)

2.4.1 General

1. All hardware and software required for the system to operate are to be installed as per manufacturer's specifications.
2. The protected space shall be provided with a complete intrusion alarm system. Intrusion protection shall be provided by way of door contact switches, and motion sensors (Note: glass break detectors used only in consultation with the Health Organization). The intrusion alarm system is designed to detect unauthorized entry into protected spaces.
3. The intrusion alarm system may be divided into separate partitions.
4. The intrusion alarm control panel shall have a sufficient number of zone inputs so that each device shall be connected to a single zone (double doors may be grouped as a single zone).
5. Home-run all devices to the alarm panel - do not gang or group devices unless otherwise authorized in writing by the Health Organization.
6. When partitioned, each partition of the intrusion alarm system shall have as a minimum the following devices:
   - Full LCD keypad
   - Siren (where required by the Health Organization)
7. The panel shall be non-proprietary (i.e. available to all alarm Security Integrators).
8. The panel power transformer shall be a minimum 37 VA. It shall be hard-wired to a dedicated, non-switched source (i.e. no plug-in type transformers).
9. Battery backup shall be gel-cell type, minimum 7 Amp/Hour. Battery installation date shall be marked on the battery and labelled on the panel cover.

10. System panel boxes shall be supervised with tamper switches:
    - Single end of line (EOL) resistors to be used.
    - Double end-of-line supervision may be required in elevated risk installations (e.g. nuclear hot labs, animal research facilities, etc.), to be determined by Health Organization.
11. EOL devices shall be installed at the device.
12. A copy of the zone descriptors shall be left inside the alarm panel.
13. Fire rated plywood backing required for all panels.
14. Installation includes field equipment, mounting hardware, wiring, terminations and I/O modules required to support the various alarm points and/or alarm systems, programming and setup of all field devices.
15. Sirens required in all settings other than acute sites.
16. Devices must be ULC approved for commercial use.
17. Acceptable manufacturer, required system components and Health Organization supplied equipment may be site specific and outlined in the attached appendices.
18. The control panel to be sized by the Security Integrator and to include an additional 20% capacity.

2.4.2 Elevated Risk Areas

1. Where controlled substances are stored and left unattended in medical units outside of Pharmacy (e.g. Day Care Surgery which may be closed at night), regardless of whether the items are stored in a dispensing unit (Pyxis), cupboard, drawer or other, an intrusion detection system is required for all installations.

2.4.3 Keypads and Panels

1. All keypads shall be LCD alpha (full English) type (unless otherwise specified).
2. All keypad emergency and quick function buttons shall be disabled.
3. All keypads to be installed at 1500mm AFF.
4. Panel mounting height, should be between 4 ft. and 8 ft. (1220mm-2440mm maximum.
5. Panels securely fastened to walls with fire rated plywood backing sufficient to support weight, including battery.
6. Proper grounding as per manufacturer's specification.
7. Panels to be screwed closed.
8. All panel installation locations to be determined in consultation with VCH PS and PHSA IMITS.

9. Acceptable manufacturer: DSC.

2.4.4 Sirens/Strobes

1. The system may include sufficient interior alarm siren to provide an audible alarm warning throughout the protected space.
    - More than one siren may be required.
    - Sirens to be minimum 100 decibels and not to exceed 120 decibels;
    - Sirens shall be programmed for 4 minute bell duration.
2. An exterior (blue) strobe shall be installed for all systems where required; strobe shall provide staff with a warning that the alarm system has been activated.
    - Strobe location to be determined in consultation with the Health Organization.
    - Strobe may be mounted inside a window within the protected space provided the strobe is visible from the exterior of the building).
    - Strobe shall be latched so that the panel must be reset to turn it off.

2.4.5 Motion Detectors

1. Motion detectors shall only be dual technology type (PIR and microwave).
2. All motion detectors to be installed at manufacturers recommended height.
3. All motion detectors shall be field-adjusted as per manufacturer's specifications for full coverage pattern of the protected spaces. Dual tech 360° detectors may be installed where applicable.
4. Devices must be ULC approved for commercial use.

2.4.6 Glass Break Detectors/Shock Sensors

1. If approved for use, all devices shall be installed and field-adjusted, tested and commissioned as per manufacturer's specifications.
2. Devices must be ULC approved for commercial use

2.4.7 Door/Window Contacts

1. Every door which leads to the protected space shall be fitted with a door contact switch.
2. All grade level or easily accessible opening windows shall be equipped with a contact.
3. All door contacts shall be installed at the top of the door, opposite the hinge side of the door.

4. All door and window contacts must be “wide gap” type.
5. All door and window contacts must be concealed unless otherwise directed. If installed in wood or similar material, allow for expansion. Fill all voids with RTV silicone or equivalent.
6. Where access and intrusion door contacts are required, they are to be wired separately to their respective panels/controllers; use of a DPDT contact is required.
7. DPDT contacts are reserved for security systems only
8. Devices must be ULC approved for commercial use.

2.4.8 Monitoring

1. The Health Organization retains the right to monitor their alarm systems in the manner of their choice and shall not be locked into any other monitoring arrangements as a result of alarm system installations.
2. Security Integrator shall provide to the Health Organizations’ authorized monitoring agent/station in order to facilitate a security response. Costs for setup and coordination, if applicable, are the responsibility of the Security Integrator.
3. Where applicable, ethernet cabling to be installed by PHSA and to be dedicated to the alarm system.
4. Alarm panels are to be programmed for remote administration by the Health Organization and the security response company as identified by the Health Organization.

2.4.9 Ethernet

1. Utilize the health care network for Ethernet alarm communications to the monitoring station.
2. Requires the use of the DSC Power Series Neo LTE/HSPA/Internet Cellular/Dual Path Alarm Communicator LE2080(R)E/TL280LE(R)E which is approved on the Health Organizations Network.

2.4.10 Cellular Communication (GSM)

1. GSM is required for monitoring of control panels with panic/duress and/or critical function devices (e.g. blood bank, vaccine fridges/freezers) unless specified by the Health Organization.
2. For intrusion only panels, GSM is only required at community sites and elevated risk areas as deemed by the Health Organization (e.g. pharmacies, hot labs, etc.).
3. GSM shall only be used as a backup method for monitoring unless approved in writing by the Health Organization.

4. Sites monitored solely by GSM, either temporary or permanent, shall have active supervision.
5. GSM that is required for existing security systems' and/or upgrades is at the discretion of the Health Organization.
6. GSM modules shall transmit all signals from the control panels to the monitoring station.
7. GSM downloading must be enabled and functional on all panels.
8. Devices must be ULC approved for commercial use.

2.4.11 Intrusion System Programming

1. The Security Integrator shall be responsible for all programming of the alarm system. This includes all user codes, all zone definitions and establishing a connection to the Health Organizations' monitoring station.
2. Zone descriptors and naming conventions to be approved by VCH PS.
3. The Health Organization shall supply the Security Integrator with all access codes and IP addresses to be programmed into the alarm system.
4. The panel shall be programmed in SIA format, unless otherwise approved by the Health Organizations.
5. The Security Integrator shall program the following:
   - Daily test transmission.
   - Bell time-out shall be set at 4 minutes.
   - Auto closing times.
   - Remote download access enabled and functional.
   - Access & panel upload codes never to be left at default.
   - Installer and master codes to be provided to VCH PS only.
6. The Security Integrator shall not install a contractor's lockout enable and shall not program Forced Arming without prior approval from the Health Organization. Auto disarming is never to be enabled.
7. Upon completion of programming, the installer shall coordinate an upload of the panel programming with the Health Organizations' authorized monitoring agent.
   - Integrator to provide VCH PS with confirmation of upload in writing as soon as complete.
8. Once the system installation is completed, the Security Integrator shall not access the system either physically or electronically without the Health Organizations' approval.

2.5 Overdose Detection Technology (ODT)

2.5.1 Applications for use

1. Overdose Detection Technology (ODT) is placed in quiet, often isolated public spaces—such as washrooms—where someone might experience a medical emergency without anyone noticing. The technology helps identify when a person becomes unresponsive in these spaces so that help can be sent quickly.
2. ODT may be used in other applications where basic environmental monitoring may be required. Requires approval from VPS.

2.5.2 General

3. All hardware and software required for the system to operate are to be installed as per manufacturer's specifications and VCH Security Technology standards.
4. All ODT parts shall be physically connected and not utilize any wireless technology. All wireless considerations shall be approved by VPS.
5. Where ODT device and cloud licensing is required to for the solution design to function, these licenses shall be included with the device.
6. Reference Sections
    a. Access Control System (ACS) system standards section 2.2
    b. Video Surveillance System (VSS) system standards section 2.3
    c. Intrusion Detection System (IDS) system standards section 2.4
7. Each installation is a custom solution that may vary from location to location. As a result, all ODT solutions and workflows must be approved by VPS.
8. ODT's are for indoor use ONLY and may not be considered in areas where there is significant airflow is present.
9. ODT's may not work as desired in areas some areas including where people might sleep and/or near approved activities that may produce dust, smoke (aka smudging), and steam etc.

2.5.3 Monitoring and Integrations

1. Alarm monitoring is via the sites/area Intrusion Detection System (IDS). New IDS system may be required if existing system is not present/sufficient.
2. IDS output to VCH Regional Access Control System (ACS) alarm monitoring platform where present. New ACS head end may be added if not present/sufficient and deemed necessary by VPS.
3. Cloud Dashboard required for Admin functions and secondary monitoring.
4. Alarm reporting destinations:
    a. VCH Protection Services Security Operations Centre
    b. On site Security first responders (where present & appropriate)
    c. On site Clinical first responders (where present & appropriate)

5. Video Surveillance System (VSS) – Integration with the VSS may be considered but requires approval from VPS.

2.5.4 Installation

1. PoE Network switch ports, wiring, and programming must be provided by the Health Organization. All ODT's shall be connected to the healthcare network.
2. Network configuration, firewall, VLAN, etc to be configured to allow the cloud subscription/service to be utilized.
3. No assumptions to me made. If the scope of work or end result is not clear, then the installing vendor must seek clarity to ensure the installation is correct and to the customer specifications.
4. Each installation is a custom solution that may vary from location to location. As a result, all ODT solutions and workflows must be approved by VPS.
5. Cloud dashboard – All devices are required to connect to the cloud dashboard.
6. ODT Device(s) – strategically placed inside the room/area of concern, ensuring appropriate coverage.
7. Strobe light(s) – strategically placed outside the room of concern. Single strobe light for group of ODT rooms is acceptable when it makes sense to do so and is approved by VPS.
8. Strobe lights(s) – strategically placed in locations to alert first responders of an alarm condition being present to act.
9. Key switch(s) – strategically placed near the room(s) of concern to silence/reset the device
10. Keypad(s) – strategically placed to serve as alarm annunciator (where required) and can also be used to reset/silence.
11. Intrusion Detection System (IDS) – ODT devices to be connected to IDS system. Each device to have its own zone and reside on an ODT partition.
12. Access Control System (ACS) – Intrusion detection system integrated with the regional ACS alarm monitoring system where present in the building.
13. Video Surveillance System (VSS) – Integration with the VSS may be considered but requires approval from VPS.
14. Halo device settings & LED colors:
    a. THC – Green
    b. Smoking/Vape - Violet
    c. Overdose detection/unconscious person - Blue
    d. Tamper - Red
    e. Help call - Cyan
    f. Aggression – White
    g. Masking – Yellow

15. Help call key words to be determined at the time of install, if used. VPS to determine if this feature to be used and what the key words are to be.
16. Signage – Appropriate VCH approved ODT monitoring signage is required outside each room to indicate health and safety monitoring is in progress.

2.5.5 Standard of Acceptance – Approved ODT & support devices

1. Motorola Halo Smart Sensor 3C-PC
2. Motorola Halo Smart Sensor 3C (for use with HALO-AMP-OS)
3. Motorola Halo Amp HALO-AMP-OS
4. BLUE Strobe (STI SA5000-B)
5. Camden CM-1200-60KA series key switch is installed to silence/reset the system.
6. Alarm keypad – As per IDS section
7. Connection to Health Authority network
8. Halo Cloud Subscription/licence
9. VCH ODT Signage – Approved graphic available from Protection Services. Signs ordered from VGH Print Shop

2.6 Panic/Duress Systems

2.6.5 General

2.6.5.1 A duress alarm is an activation device placed covertly and accessible which is intended for security situations where silent notification is appropriate. Typical locations include cash handling areas, pharmacy, reception, and administration.

2.6.5.2 A panic alarm is an activation device placed overtly and accessible which is intended for security situations where silent notification is not required.

2.6.5.3 All hardware and software required for the system to operate are to be installed as per manufacturer's specifications.

2.6.5.4 Panic/duress alarms shall be activated by a hardwired button(s) or wireless button(s)/transmitter(s) as required.

2.6.5.5 Interior duress buttons to be mounted covertly under counter/desk or wall mounted.

2.6.5.6 Interior panic buttons to be mounted overtly on wall; VCH PS approval required for under counter/desk.

2.6.5.7 Exterior panic buttons to be wall mounted or pole mounted.

2.6.5.8 All wall or pole mounted buttons to be an internally illuminated button.

2.6.5.9 Where applicable, the hard wired and wireless systems shall enunciate on the same platform/display.

2.6.5.10 All wall mounted fixed buttons to be mounted at 48" CL AFF unless otherwise noted.

2.6.5.11 Placement of under counter buttons to be approved by VCH PS prior to installation.

2.6.5.12 Panic/duress buttons to be strategically located and identified/clearly labeled for "security emergency".

2.6.5.13 Protective covers to be installed on wall or pole mounted buttons unless otherwise specified by the Health Organization.

2.6.5.14 All panic/duress buttons located on movable furniture shall be connected using an RJ 12 wall jack and a telephone patch cord to the jack. The wall jack shall be clearly identified by a label marked "Panic System" (lamacoid or other professional label).

2.6.5.15 Wireless buttons affixed in place is not an acceptable installation method.

2.6.5.16 System panel boxes shall be supervised with tamper switches:

- Single end of line (EOL) resistors to be used.
- Double end-of-line supervision may be required in elevated risk installations (e.g. nuclear hot labs, animal research facilities, etc.), to be determined by Health Organization.

2.6.5.17 EOL devices shall be installed at the device.

2.6.5.18 Acceptable manufacturer required system components and Health Organization supplied equipment may be site specific and outlined in the attached appendices.

2.6.6 Elevated Risk Areas

2.6.6.1 Where controlled substances are stored outside of pharmacy, regardless of whether the items are stored in a dispensing unit (Pyxis), cupboard, drawer or other, immediate proximity to a duress button (e.g. in the same room) is required for all installations.

2.6.7 Devices

2.6.7.1 All hardwired panic/duress buttons must be latching.

2.6.7.2 Acceptable manufacturers: Under counter buttons: USP HUB2B; Wall buttons: STI-USA Model SS2229ZA-EN with custom features including cover and custom label of "Security Emergency".

2.6.8 Monitoring

2.6.8.1 The Health Organization retains the right to monitor their alarm systems in the manner of their choice and shall not be locked into any other monitoring arrangements as a result of alarm system installations.

2.6.8.2 Security Integrator shall provide ethernet connectivity (hardware & software) to the Health Organizations' authorized monitoring agent/station in order to facilitate a security response. Costs for setup and coordination, if applicable, are the responsibility of the Security Integrator.

2.6.8.3 Where applicable ethernet to be installed by PHSA.

2.6.8.4 Alarm panels are to be programmed for remote administration by the Health Organization and the security response company as identified by the Health Organization.

2.6.9 Ethernet

2.6.9.1 Utilize the health care network for Ethernet alarm communications to the monitoring station.

2.6.9.2 Requires the use of the DSC Power Series Neo LTE/HSPA/Internet Cellular/Dual Path Alarm Communicator LE2080(R)E/TL280LE(R)E which is approved on the Health Organizations Network.

2.6.10 Cellular Communication (GSM)

2.6.10.1 GSM is required for monitoring of control panels with panic/duress and/or critical function devices (e.g. blood bank, vaccine fridges/freezers) unless specified by the Health Organization.

2.6.10.2 GSM shall only be used as a backup method for monitoring unless approved in writing by the Health Organization.

2.6.10.3 Sites monitored solely by GSM, either temporary or permanent, shall have active supervision.

2.6.10.4 GSM that is required for existing security systems' and/or upgrades is at the discretion of the Health Organization.

2.6.10.5 GSM modules shall transmit all signals from the control panels to the monitoring station.

2.6.10.6 GSM downloading must be enabled and functional on all panels.

2.6.10.7 Devices must be ULC approved for commercial use.

2.6.11 Local Response Panic/Duress Systems (Not Monitored)

2.6.11.1 Where specified, install a local response panic/duress system which is not externally monitored for a security response.

2.6.11.2 When the panic alarm push button is pressed, a flashing amber light and chime (or other unique audible signal) shall sound in a remote designated area (acceptable product: STI-USA SA5000A).

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

2.6.11.4 Each standalone panic alarm panel shall be controlled by an LCD keypad that shall clearly identify the location of each panic button.

2.6.11.5 Acceptable manufacturers are site specific and outlined in the attached appendices.

2.6.12 Monitored Panic Alarm Systems

2.6.12.1 VCH PS Services and the client is to be consulted as to whether or not monitored panic buttons shall also report locally.

2.6.12.2 Acceptable manufacturers are site specific and outlined in the attached appendices.

2.6.13 Wireless Panic Alarm Systems

2.6.13.1 Wireless panic alarms shall only be installed at the direction of the Health Organization.

2.6.13.2 All wireless panic alarms must be tested throughout the entire protected area so as to ensure that the panic buttons work in all locations.

2.6.13.3 Acceptable manufacturers are site specific and outlined in the attached appendices.

2.6.13.4 RTLS monitoring workstation(s) to be provided by the Security Integrator unless otherwise specified by the Health Organization.

2.6.14 Panic / Duress System Programming

2.6.14.1 Required programming includes, but is not limited to, device enrollment and programming, labeling/naming all devices, graphic user interface, and client software/user setup.

2.6.14.2 Electronic versions of floor plans, if required, to be supplied by the Health Organization.

2.6.15 Integration Requirements

2.6.15.1 Other security systems may be integrated into Panic/Duress Systems. This will be determined on a case by case basis and written approval from VCH PS is required prior to any integration.

2.7 Intercom Systems

2.7.5 General

2.7.5.1 All hardware and software required for the system to operate are to be installed as per manufacturer's specifications.

2.7.5.2 Where required, intercoms/intercom systems shall be installed for communications.

2.7.5.3 Unless otherwise specified, video intercoms shall be utilized.

2.7.5.4 The client may elect to have the intercom integrated with the entry door controls and/or the access control/card reader system for remote door control. The Security Integrator is responsible for all interfacing between the various systems.

2.7.5.5 Point to point/hard wired intercom to be used unless otherwise specified.

2.7.5.6 IP-based /intercoms may be utilized in certain conditions and must be approved, in writing, by the VCH PS.

2.7.5.7 Intercoms to be installed at height recommended by the manufacturer. Where no manufacturer recommendations exist height of door station to be approved by VCH PS.

2.7.5.8 Acceptable manufacturer required system components and Health Organization supplied equipment may be site specific and outlined in the attached appendices.

2.7.6 Devices

2.7.6.1 Intercom camera to be minimum 180 degree field of view (FOV).

2.7.6.2 Approved manufacturers: Aiphone or approved equivalent.

2.7.7 Intercom System Programming

2.7.7.1 Program the system and associated components to the satisfaction of the VCH PS.

2.7.7.2 Required programming includes, but is not limited to, labeling/naming all devices and client software/user setup.

2.8 Asset Protection Technologies (APT)

2.8.5 General

2.8.5.1 Asset Protection Technologies standards such as property, Infant, & Patient are currently in development.

2.8.5.2 Contact VPS for more information

2.9 Concealed Weapons Detection Technology (CWD)

2.9.5 General

2.9.5.1 Concealed Weapons Detection Technology standards in development

2.9.5.2 CWD to be considered in all new development and renovations, including space.

2.9.5.3 Contact VPS for more information

2.10 Integration Engine

2.10.5 General

2.10.5.1 An integration engine is a software platform that is designed to integrate and process data between numerous healthcare systems.

2.10.5.2 Security system(s) may be incorporated in an integration engine for the purposes of reporting, data processing and event alert(s)/notification(s).

2.10.5.3 The integration engine cannot control or compromise security system integrity and/or functionality.

3.0 Area/Site Specific Requirements

3.1 Under Construction

3.1.1 General

3.1.1.1 Contact VPS for more information about area specific physical and security system specific requirements.

Glossary of Terms

Access Control: The act of controlling the entry and egress from a building or area, by validating a credential or an individual. Access control is the selective restriction of access to a place or other resource while access management describes the process. Permission to access a resource is called authorization.

Audit Trail: A system that traces the detailed transactions related to any item in a database, file or record.

Authorities Having Jurisdiction (AHJ): Authorities that have jurisdiction over a location, resource, procedure etc.

Crime Prevention Through Environmental Design (CPTED): CPTED emphasizes the impact of proper design and effective use of a built environment, such that the facility can reduce the opportunity and fear of predatory type of crime and enhance the quality of life (or the safe and secure experience of the health-care environment). CPTED is particularly applicable to VCH because of the diverse users and mix of uses in these types of facilities. Incorporating CPTED can significantly reduce the opportunity, fear, and risk of crime. In addition, CPTED mitigation strategies can reduce costs associated with adding subsequent security equipment and security personnel, after an incident has occurred.

Canadian Standards Association (CSA): CSA Group's not-for-profit Standards organization that is to enhance the lives of Canadians through the advanced standards in public and private sectors. A leader in standards research, development, education, and advocacy.

Duress Alarm: An activation device placed covertly and accessible which is intended for security situations where silent notification is appropriate. Typical locations include cash handling areas, pharmacy, reception, and Administration.

Electronic Access Control (EAC): A method of access control that uses computer-based technology to control and monitor access.

Emergency Department (ED): Usually as part of a larger HCF, the Emergency Department is a medical treatment facility specializing in emergency medicine and provides acute care treatment of patients that arrive by various means without prior appointment.

Electronic Infant Monitoring System: an electronic security system designed to enhance the safety of infants in obstetric and pediatric departments. Such systems may include a small, tamper-proof tag to be placed on the infant after birth. Should an infant be carried toward an exit door, the system could initiate a security response which may include setting off an alarm, activating door locks and holding selected elevators.

Elevated Risk Area (ERA)
Elevated risk areas are locations or situations that present a higher probability of hazards, contamination, or harm compared to other areas.

Elevated Risk Area Assessment (ERAA): is a systematic evaluation of certain areas and departments within healthcare facilities that are designated as "Elevated Risk Areas", and its security measures. The goal is to identify potential vulnerabilities and areas for improvement. The ERAA is carried out by VCH Protection Services and/or delegate.

Healthcare Facility (HCF): Any VCH facility involved in providing healthcare service or treatment simultaneously to four or more patients who may be primarily incapable of self-preservation due to physical or mental limitation; or who are undergoing treatment or testing which may temporarily render a patient incapable of taking effective action under emergency conditions without assistance from others.

Infection Control Risk Assessment (ICRA): Developed by the CSA, the ICRA determines the preventive measures required and intended to protect patients and building occupants from disease transmission and other health problems, such as allergic reactions, that can be produced by the construction, renovation, or maintenance of health care facilities.

Intrusion Detection System (IDS): A system combining mechanical or electric components to perform the functions of sensing, controlling, and announcing unauthorized entry into areas covered by the system. The IDS is intended to sound alarms or alert response personnel to an actual or attempted intrusion into an area.

Integrated System: An approach that integrates some or all of an organization’s systems, enabling it to review data comprehensively and work more effectively as a single unit with unified objectives.

Long-Term Care Facility (LTC): A facility that provides rehabilitative, restorative, and/or ongoing skilled nursing care to patients or residents in need of assistance with activities of daily living. Long-Term Care facilities include nursing homes, skilled nursing facilities, and assisted living facilities and provide a variety of services, both medical and personal care, to people who are unable to manage independently in the community.

Network Video Recorder (NVR): is a specialized computer that records security video surveillance footage in digital format to a hard drive. Often referred to as a CCTV server or appliance.

Panic Alarm: An activation device placed overtly and accessible which is intended for security situations where silent notification is not required. Typical locations include ICU, Behavioral health, Emergency Department, and parking areas.

Physical Security Risk Assessment (PSRA): is a systematic evaluation of a department within a healthcare facility, and/or the entire healthcare facility, and its security measures, with the goal of identifying potential vulnerabilities and areas for improvement. The PSRA is carried out by VCH Protection Services and/or delegate.

Provincial Digital Health & Information Services (PDHIS): A PHSA department/service, which comprises of all Information Technologies (IT) devices, systems, and support. May also be referred to as PHSA. Previously known as IMITS, BCCSS, & HSSBC.

Provincial Health Services Authority (PHSA): is a publicly funded health service provider in the province of British Columbia. PHSA is unique in Canada as the only health authority having a province-wide mandate for specialized health services.

Protected Health information (PHI): Any information about health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual.

Protective Glazing Material: Is used to counter many threats to buildings and occupants including bomb (blast) attacks, ballistic attack, burglary or robbery incidents, forced entry, detention containment, and natural disasters such as seismic occurrences, hurricanes and tornadoes. The proper choice of security glazing is dependent on understanding the desired level of protection, and functional requirements as determined from the SVA.
RFI – Request for Information

Radio Frequency Identification (RFID): The electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum used to transmit signals. An RFID system consists of an antenna and a transceiver, which reads the RF and transfers the information to a processing device and a transponder or tag, which is an integrated circuit containing the RF

circuitry and information to be transmitted; an emerging technology that enables companies to better track assets, tools and inventory.

Restricted Area: A room, office, building, or facility area to which access is strictly and tightly controlled. Admittance to this area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area.

Risk: The potential for uncontrolled loss, harm or damage to something of value.

Risk Assessment: The overall process of risk identification, risk analysis, risk evaluation and determination of the amount of risk that is acceptable. Note: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls. Also see

Real Time Locating System (RTLS): technologies that use wireless signals to determine the precise location of tagged assets or personnel.
Screening: Examining persons and their possessions for contraband such as weapons, explosives, and CBR agents using magnetometer, x-ray, search, or another device.

Security Systems: Any of various physical or operational means of safeguards intended as protective measures to mitigate risk to persons or property.

Security Operations Centre (SOC): Centralized call centre and security monitoring station for security operations and response.

VCH Security Design Standards (VSDS): The security design standards for Vancouver Coastal Health. This document.

Vancouver Coastal Health (VCH): Vancouver Coastal Health is a regional health authority that provides health services including primary, secondary, tertiary and quaternary care, home and community care, mental health services, population and preventive health and addictions services in part of Greater Vancouver and the Coast Garibaldi area.

VCH Protection Services (VPS): The corporate Security department/program for Vancouver Coastal Health.

Video Intercom System: A solution that allows one to electronically see and talk with individual(s) before admitting them into the facility. By determining a visitor's identity before unlocking the door, one can avoid face-to-face confrontation with a possible dangerous individual.

Video Surveillance: A system of monitoring activity in an area or building using one or more video cameras on a network which can capture video, and possibly audio information. Signals are not publicly distributed and sent to a defined place to be monitored for security or other purposes. Digital video surveillance systems can be used for nearly any environment, and stored and replayed for forensic evidence, or serve as a crime prevention tool. Historically referred to as Closed Circuit Television (CCTV).