Electronic Security Systems Standards

Version 1.0 - June 2024

Vancouver CoastalHealth

Electronic Security Systems Standards © Vancouver Coastal Health

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

Please contact your VCH Protection Services Representative or ProtectionSystems@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

1.0 General Requirements

1.1 Overview Documents

1.1.1. This document outlines Electronic Security System requirements for all hospitals and/or healthcare facilities with in Vancouver Coastal Health (VCH). Applicable sites are listed in Section 1.2. Sites may not be specifically listed due to security, safety and/or other reason(s). For Electronic Security Systems requirements for sites not listed, contact VCH Protection Services (VCH PS).

1.1.2. The VCH Protection Services Department (VCH PS) oversees Electronic Security Systems Specifications (ESSS) 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 VCH PS.

1.1.3. This document outlines Vancouver Coastal Health's ESSS for the following:

- Electronic Access Control Systems
- Close Circuit Television (CCTV)/Surveillance Systems
- Intrusion Alarm Systems
- Panic / Duress Alarm Systems [(including Real Time Locating Systems (RTLS)]
- Intercommunication Systems
- Other Security Technologies, such as, but not limited to weapons detection.

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 VCH PS to ensure required functionality is achieved.

1.1.4. 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.
- Section 3 - Appendices: Lists specific requirements at each site - such as acceptable manufacturers, Health Organization supplied equipment, operational response communication method.

1.1.5. Systems standards are constantly evolving and being updated. Consultants and vendors should contact VCH PS for confirmation of design.

1.2 Applicable Sites

Acute Care SIte	
Richmond Hospital (RH) 7000 Westminster Highway Richmond, BC V6X 1A2 See Appendix 1 for site specific requirements	Squamish General Hospital (SGH) 38140 Behrner Drive Squamish, BC V0N 3G0 See Appendix 5 for site specific requirements
Lion's Gate Hospital (LGH) 231 East 15th Street North Vancouver, BC V7L 2L7 See Appendix 2 for site specific requirements	Sechelt Hospital (SH) 5544 Sunshine Coast Highway Sechelt, BC V0N 3A0 See Appendix 6 for site specific requirements
Vancouver General Hospital (VGH) 855 West 12th Avenue Vancouver, BC V5Z 1M9 See Appendix 3 for site specific requirements	qathet General Hospital (qGH) 5000 Joyce Avenue Powell River, BC V8A 5R3 See Appendix 22 for site specific requirements
University of British Columbia Hospital (UBCH) 2211 Wesbrook Mall Vancouver, BC V6T 2B5 See Appendix 4 for site specific requirements	

Non-Acute Care Sites	
Whistler Health Care Centre 4380 Lorimer Road Whistler, BC V8E 1A7 Contact VCH PS for site specific requirements	Pemberton Health Centre 1403 Portage Road Pemberton, BC V0N 2L0 Contact VCH PS for site specific requirements
Bella Coola General Hospital 1025 Elcho Street Bella Coola, BC V0T 1C0 Contact VCH PS for site specific requirements	R.W. Large Memorial Hospital 88 Waglisla Street Bella Bella, BC V0T 1Z0 Contact VCH PS for site specific requirements
Contact your VCH PS Representative or contact PStechsupprt@vch.ca	

1.3 Related Documents

1.3.1 Privacy Guidelines – Freedom of Information and Protection of Privacy Act (FOIPP).

- http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

1.3.2 Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies.

- https://www.oipc.bc.ca/resources/guidance-documents/

1.3.3 The Health Organization' Cabling Standards. Cabling to be installed to PHSA standards.

- Contact PHSA for current version of *"Cabling Standards"*.

1.3.4 CSA and Health Organization Infection Control Standards.

- https://www.csagroup.org/
- https://ipac-canada.org/

1.3.5 International Association of Healthcare Security and Safety Basic (IAHSS) Industry Guidelines

- http://www.iahss.org

1.3.6 BC Security Services Act

- https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/07030_01

1.4 Reference Standards

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

1.4.1.1 Canadian Electrical Code (CEC) Part 1 C22.1-00. BC Amendments to the CEC & associated bulletins.
1.4.1.2 BC Electrical Safety Act.
1.4.1.3 British Columbia Building Code.
1.4.1.4 British Columbia Fire Code Regulation.
1.4.1.5 TIA/EIA 568-B.1 through B.3 Commercial Building Telecommunications Cabling Standards.
1.4.1.6 TIA/EIA 569- B Commercial Building Standard for Telecommunications Pathways and Spaces.
1.4.1.7 ANSIA/TIA/EIA - 607A (J-STD-607-A-2002) Commercial Building Grounding and Bonding.
1.4.1.8 NEMA – National Electrical Manufacturers Association
1.4.1.9 Work Safe BC, Workers Compensation requirements.

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

1.5 Standard Requirements

1.5.1 Security Integrator(s) field staff and programmers shall be fully trained, and factory certified on all security systems as required.

1.5.2 All equipment shall remain the sole property of the Health Organization and the installing company shall not retain ownership or control of the system.

1.5.3 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.

1.5.4 Panels, computers and other devices are not to be locked out (e.g. vendor supplied locking devices, electronically by password, etc.)

1.5.5 Provide all passwords to VCH PS, including installer, administrator, and the user passwords for all systems.

1.6 Licences, Approvals, Permits & Standards

1.6.1 The Security Integrator shall be responsible for all building and electrical permits, licenses, inspections and related fees as required.

1.6.2 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.

1.6.3 On site Facilities Maintenance & Operations (FMO) and/or other health organization contacts are required to be consulted prior to the commencement of any work.

1.6.4 The Security Integrator and all workers must be provincially licensed and/or meet all requirements outlined as legislated in the BC Security Services Act.

1.6.5 The VCH PS Department oversees Electronic Security Systems within the Health Organizations 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 VCH PS.

1.7 Products

1.7.1 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.

1.7.2 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 the health organization.

1.7.3 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.

1.7.4 Referenced manufacturers' products have been approved as standard equipment for installation at the Health Organizations' facilities and shall not be substituted or replaced with non-approved alternates without written approval from the VCH PS representative.

1.7.5 Acceptable manufacturers may be site specific and outlined in the attached appendices.

1.8 Operational Requirements Including Response

1.8.1 Electronic security systems installed in the Health Organizations' facilities shall operate on a 24-hour basis throughout the year.

1.8.2 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.

1.8.3 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.

1.8.4 Security systems may require a local response from the contracted security service provider on site (where applicable). Methods for communicating system alarms and notifications vary from site to site. Refer to the attached appendices to determine the required *operational response communication method*.

1.9 System Conductors and Cables

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

1.9.2 All camera installations to be IP/Networked based. Exceptions (e.g. analog cameras) require written VCH PS approval.

1.9.3 All IP/Networked cabling required for CCTV installations must follow the Health Organization's structured cabling standard and must be installed by an authorized

structured cabling vendor. Please contact the Health Organization for the most recent version of the Structured Cabling Specification.

1.9.4 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).

1.9.5 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.

1.9.6 All wiring shall be concealed unless otherwise authorized, in writing, by the Health Organization.

1.9.7 Video Signal Cabling for analogue devices for interconnection between equipment shall be minimum RG-59 type, solid bare copper center conductor with minimum 95% copper braid shield. For cable runs over 300 meters in length, RG-6 cable should be used. All CCTV coaxial cable connections shall be made using crimped or pre- manufactured connectors only, twist on connectors are not permitted. Cat 6 and video baluns are acceptable.

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

1.9.9 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, stakons or approved equivalent (Marrette connectors are not allowed).

1.10 Computers, Software and Software Related Licensing

1.10.1 Computers, servers, printers and other supporting peripheral equipment may be required as outlined in these specifications.

1.10.2 Hardware, computers, servers, printers and other supporting peripheral equipment, as required, can be provided by either the Security Integrator or the Health Organization; to be determined on a case by case basis.

1.10.3 The Security Integrator is required to ensure that all software versions provided are equivalent to the software currently in use by the Health Organization.

1.10.4 Security Integrators supplied equipment to meet or exceed Health Organization requirements, where applicable.

1.10.5 Security Integrators are required to determine in advance, which equipment shall be supplied by the Health Organization/PHSA, and which equipment shall be required to be supplied by the Security Integrator.

1.10.6 Where required, software/software licenses and any other required licensing is to be supplied by the installer/Security Integrator unless otherwise stated, including all software required for Health Organizations’ supplied hardware and equipment.

1.10.7 Door/reader and other licenses required for Lenel access systems shall be supplied by the Health Organization for installations up to and including 32 doors.

1.10.8 Door/reader and other licenses required for Lenel access systems shall be supplied by the Security Integrator/installer for installations exceeding 33 doors by carrying a cash allowance (based on MSRP) for licensing being provided by the Value Added Reseller (VAR) of record.

1.10.9 Licenses purchased by Security Integrators/installers to be a minimum of 64 readers.

1.11 Coordination of Work

1.11.1 Installation Security Integrator(s) shall coordinate work with the Health Organization and their appointed representatives to ensure systems are installed, programmed, tested, commissioning and verified fully operational to the satisfaction of the Health Organization.

1.11.2 Health Organization alarm accounts shall be monitored by identified monitoring and response agency. This includes intrusion, panic/duress and other applicable systems.

1.11.3 Coordination with PHSA may be required for computer, software and peripheral devices (including any wireless components).

1.11.4 Coordinate and cooperate with other trades, clinical staff, Infection & Prevention Control Practitioners and FMO, for timely completion of all work.

1.11.5 Work may be required to be performed outside of regular business hours to avoid disruption to the delivery of patient care.

1.12 Installation

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

1.12.2 Security Integrator shall test and commission fully operational and functional systems prior to turnover to the Health Organization. The Health Organization 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 the Health Organization.

1.12.3 All cables shall be permanently identified using ¾” (minimum) printed nylon and/or vinyl labels and listed on as-built drawings as follows:

1.12.3.1 Cable Label

- Cable number
- Device

1.12.3.2 As-Built Drawings

- Cable number
- Device
- Source
- Destination

1.12.4 Electrical panel circuit numbers shall be clearly identified on all system panels.

1.12.5 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.

1.12.6 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.

1.12.7 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.

1.12.8 Security Integrator(s) shall repair at no cost to the Health Organization, any surfaces, finishes, equipment or structures damaged by the execution of their contract to its original condition.

1.12.9 All security system control panels shall be located in a secure, accessible location. Head-end security equipment for Access Control and CCTV shall be mounted at locations designated by VCH PS. Deviation from this requires written consent from VCH PS.

1.12.10 Ground security equipment as per manufacturer's recommendations.

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

1.12.12 Health Organizations' security systems do not require conduit with the following exceptions: exposed or exterior locations or where required by other Health Organization departments and/or facility policy (FMO, IMITS).

1.12.13 All wiring shall be concealed unless otherwise authorized by the Health Organization.

1.12.14 Wall mounted devices to be secured to wall studs and/or installed with plywood backing sufficient to support device weight.

1.12.15 Ceiling mounted devices to be secured with sufficient backing to support device weight and meet seismic requirements.

1.12.16 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.

1.12.17 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 site specific information contained in the site appendices.

1.13 Programming

1.13.1 Programming of all systems to be completed in full by the Security Integrator, in consultation with VCH Protection Service.

1.13.2 Programming of all system devices and components are to be done to the satisfaction of VCH PS.

1.13.3 Access control database programming must be completed by the Health Organization's designated Security Integrator. Refer to Acceptable Security Integrator in Section 2, Electronic Security Systems. The installation contractor is to cover all associated costs of programming.

1.13.4 VCH Protection Services will provide the naming convention(s) required for the access control database programming.

1.13.5 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 site specific information contained in the site appendices.

1.14 Documentation

1.14.1 The Security Integrator shall provide the following documentation for each system to VCH PS:

1.14.1.1 All installation and user manuals are to be provided in electronic form.

1.14.1.2 Provide map overlay with the location of all devices, control panels, keypads, riser diagrams. Drawings to be provide electronically in a format suitable to VCH PS.

1.14.1.3 All zones shall be clearly identified on the as-built drawings.

1.14.1.4 Electrical panel circuit breaker shall be clearly identified and noted on both the panel cover and as-built drawings.

1.14.1.5 A printout of the monitoring company activity report that verifies full system testing in electronic form.

1.14.1.6 Device verification sign-off sheets, electronic and/or paper, if required.

1.14.1.7 Manufacturer's cut sheets for all devices, electronic and/or paper, if required.

1.14.1.8 Infection Control documentation, if required.
1.14.1.9 All forms completed as supplied by the Health organization.
1.14.1.10 Municipal and other required electrical permits.
1.14.1.11 Warranty Certificate, if required.

1.14.2 All documentation to be submitted to the health organization's designate, as required.

1.14.3 Security Integrator(s) shall provide the Health Organization 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.

1.15 Training

1.15.1 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 VCH PS), and shall be conducted at a time that is mutually agreeable to both the Security Integrator and the Health Organization.

1.16 Warranty

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

1.16.2 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.

1.17 Alarm Monitoring

1.17.1 Overview

1.17.1.1 The Health Organization may require off site ULC rated alarm monitoring service to facilitate a personnel response to system generated alarms. Refer to appendices for site and system specific off site alarm monitoring requirements.

1.17.1.2 All alarm systems and ancillary equipment shall conform to the Health Organization's Security System Specifications.

1.17.1.3 Account numbers and other applicable information shall be provided by Health Organization's authorized monitoring agent/station monitoring station.

1.17.1.4 Refer to Acceptable Security Integrators section for off-site monitoring company.

1.17.1.5 The Security Integrator is to cover all associated costs of programming and monitoring set-up, if required.

1.18 Security Integrator Responsibilities

1.18.1 All Electronic Security Systems and its related hardware and software are to be installed as per manufacturer specifications.

1.18.2 The Security Integrator shall ensure that all required information is provided and recorded on the Health Organization's authorized monitoring agent/station as required.

1.18.3 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.

1.18.4 The Security Integrator is responsible for all associated costs of programming and monitoring set-up, if required.

1.18.5 Access to the system for post installation warranty/deficiency service, or other required access, to be coordinated with VCH PS.

1.18.6 All passwords for all devices to be supplied to VCH PS.

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

1.19 Health Organization (Tenant) Responsibilities

1.19.1 Once the system is installed and commissioned the Health Organization (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 VCH PS (Health Organization's authorized monitoring agent/station).

1.19.2 All Information is to remain confidential at all times.

1.20 List of Security Integrators

1.20.1 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 Health Organization security systems.

1.20.2 Preferred Security Integrators for listed systems include:

1.20.2.1 Houle Security
https://www.houle.ca/services-and-solutions/security-life-safety/

1.20.2.2 Johnson Controls International (JCI)
https://www.johnsoncontrols.com/buildings/security-and-fire-safety

1.20.2.3 Paladin Technologies

https://paladintechnologies.com/

1.20.2.4 Centre Electrical + Technology
www.cecgrp.ca

1.20.3 Mandatory Security Integrators required for Access Control database programming:

1.20.3.1 Paladin Technologies
https://paladintechnologies.com/

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 Access Control (Card Reader) Systems

2.1.1 General

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

2.1.1.2 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.

2.1.1.3 Elevator control, where required, shall be installed to allow for control of the elevator on a floor by floor basis.

2.1.1.4 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.

2.1.1.5 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.

2.1.1.6 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.

2.1.1.7 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.

2.1.1.8 Magnetic locks are not permitted unless authorized in writing by the Health Organization.

2.1.1.9 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.

2.1.1.10 Card readers are to be proximity type.

2.1.1.11 Card readers may also be required to have PIN code authentication in addition to proximity authentication.

2.1.1.12 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.

2.1.1.13 Access control database programming must be completed by the Health Organization's designated Security Integrator. Refer to Acceptable Security Integrator section.

2.1.1.14 Acceptable manufacturer, required system components and Health Organization's supplied equipment may be site specific and as outlined in the attached appendices.

2.1.2 Card Readers

2.1.2.1 Readers shall be connected to door controller via standard Wiegand interface.

2.1.2.2 Readers shall be HID Signo unless approved in writing by VCH PS.

2.1.2.3 Readers must be capable of reading HID Corporate 1000 card format.

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

2.1.2.5 Exterior card reader shall be weather proof, designed for outdoor applications in the applicable environment.

2.1.2.6 All readers to be installed at 1.2m (46") above finished floor unless directed otherwise by the Health Organization.

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

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

2.1.2.9 Readers shall be black unless otherwise specified.

2.1.2.10 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.

2.1.3 Request to Exit (REX) Devices

2.1.3.1 REX devices shall allow egress through monitored doors without creating alarms with REX connected to bypass door alarm on exit.

2.1.3.2 REX devices to meet required functionality.

2.1.3.3 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.

2.1.3.4 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.

2.1.3.5 Latch bolt monitors cannot be used as REX devices.

2.1.3.6 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

2.1.4 Electrified Hardware

2.1.4.1 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).

2.1.4.2 Unless otherwise directed electric strikes shall fail “secure”

2.1.4.3 Acceptable manufacturers: Dependent on site standard for locks and hardware.

2.1.5 Door Contacts

2.1.5.1 All door and window contacts must be “wide gap” type.

2.1.5.2 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.

2.1.5.3 Latch bolt monitors cannot be used as door contacts.

2.1.6 Remote Door Control

2.1.6.1 Where required, designated doors shall have a control switch(es) installed to control door lock and unlock functions.

2.1.6.2 Access control workstations shall not be utilized for remote door control unless authorized in writing by the Health Organization.

2.1.6.3 The switch shall be integrated with the access control / card access system where applicable.

2.1.6.4 The switch shall be illuminated to indicate and differentiate between all status functions

2.1.6.5 Switch functions to include permanent lock; permanent unlock; momentary unlock.

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

2.1.6.7 Make and model of switch shall be approved by VCH PS.

2.1.7 Access Control System Programming

2.1.7.1 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.

2.1.7.2 Readers must not remain programmed in Facility Code Only Mode (online or offline); card programming must be card, PIN, or card and PIN only.

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

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

2.1.8 Integration Requirements

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

2.2 Closed Circuit Television (CCTV) Systems

2.2.1 General

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

2.2.1.2 Vendor supplied appliances must be authorized by the Health Organization.

2.2.1.3 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.

2.2.1.4 Cameras that are clinical or specialized in nature need to be approved by VCH PS before they can reside on the Security surveillance infrastructure.

2.2.2 CCTV Applications

2.2.2.1 CCTV systems can be utilized, but are not limited to, the following applications:

- Site Security
- General Clinical Observation

2.2.2.2 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).

2.2.3 Site Security CCTV Systems

2.2.3.1 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/

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

2.2.3.3 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.

2.2.3.4 The CCTV system shall provide recorded images of sufficient quality to be used as court evidence in Canada.

2.2.3.5 Output must be available for viewing by authorized persons at multiple locations, if required.

2.2.3.6 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.

2.2.3.7 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.

2.2.3.8 Plywood backing required for wall mount monitor installations to meet seismic requirements.

2.2.3.9 Exterior enclosures/equipment must be NEMA rated.

2.2.3.10 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).

2.2.3.11 Required system components and Health Organization supplied equipment is site specific and outlined in the attached appendices.

2.2.4 General Clinical Observation CCTV Systems

2.2.4.1 Cameras within Clinical units shall have the ability to record. Health Organization to determine which camera(s) are recorded.

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

2.2.4.3 Output must be available for viewing by authorized persons at multiple locations, if required.

2.2.4.4 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.

2.2.4.5 Indoor/outdoor camera enclosures must be vandal resistant domes constructed of high impact polycarbonate material or approved equipment.

2.2.4.6 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.

2.2.4.7 Exterior enclosures/equipment must be NEMA rated.

2.2.4.8 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).

2.2.4.9 Required system components and Health Organization supplied equipment is site specific and outlined in the attached appendices.

2.2.5 Elevated Risk Areas

2.2.5.1.1 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.

2.2.6 Artificial Intelligence (AI) and Video Analytics

2.2.6.1 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.

2.2.7 Cameras

2.2.7.1 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”.

2.2.7.2 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.

2.2.7.3 Cameras that are subject to extreme low light conditions must be equipped with infrared illuminators.

2.2.7.4 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)

2.2.7.5 The outdoor camera shall offer protection against the elements. The camera’s operating temperature range shall be -30° to 50° Celsius

2.2.7.6 All camera shall operate on POE, POE+ and POE++ require network switch compatibility.

2.2.7.7 Where IP cameras are installed; all cameras and converters shall integrate with site specific recording platform.

2.2.7.8 Non IP camera connections shall be crimped.

2.2.7.9 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.

2.2.8 <u>Video Recording System and Storage</u>

2.2.8.1 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.

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

2.2.8.3 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.

2.2.8.4 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).

2.2.8.5 Data storage days to be calculated utilizing RAID 6 for acute sites, unless otherwise approved by VCH PS.

2.2.8.6 NVR's must have the ability to output to a USB removable media drive.

2.2.8.7 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.

2.2.8.8 Devices to be fully programmed to provide suitable recording times (as per client requirements).

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

2.2.9 Monitors

2.2.9.1 Monitors shall be wall, ceiling or desk mounted as per the Health Organizations' requirements.

2.2.9.2 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.

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

2.2.10 CCTV System Programming

2.2.10.1 Required programming includes, but is not limited to, labeling/naming all devices (as per Health Organization naming convention) and client software/user setup.

2.2.10.2 Where available in the CCTV system, device mapping is required unless otherwise stated by VCH PS.

2.2.11 Integration Requirements

2.2.11.1 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.

2.3 Intrusion Alarm Systems

2.3.1 General

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

2.3.1.2 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.

2.3.1.3 The intrusion alarm system may be divided into separate partitions.

2.3.1.4 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).

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

2.3.1.6 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)

2.3.1.7 The panel shall be non-proprietary (i.e. available to all alarm Security Integrators).

2.3.1.8 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).

2.3.1.9 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.

2.3.1.10 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.

2.3.1.11 EOL devices shall be installed at the device.

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

2.3.1.13 Fire rated plywood backing required for all panels.

2.3.1.14 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.

2.3.1.15 Sirens required in all settings other than acute sites.

2.3.1.16 Devices must be ULC approved for commercial use.

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

2.3.1.18 The control panel to be sized by the Security Integrator and to include an additional 20% capacity.

2.3.2 Elevated Risk Areas

2.3.2.1 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.

2.3.3 Keypads and Panels

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

2.3.3.2 All keypad emergency and quick function buttons shall be disabled.

2.3.3.3 All keypads to be installed at 1500mm AFF.

2.3.3.4 Panel mounting height, should be between 4 ft. and 8 ft. (1220mm-2440mm maximum.

2.3.3.5 Panels securely fastened to walls with fire rated plywood backing sufficient to support weight, including battery.

2.3.3.6 Proper grounding as per manufacturer's specification.

2.3.3.7 Panels to be screwed closed.

2.3.3.8 All panel installation locations to be determined in consultation with VCH PS and PHSA IMITS.

2.3.3.9 Acceptable manufacturer: DSC.

2.3.4 Sirens/Strobes

2.3.4.1 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.

2.3.4.2 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.

2.3.5 Motion Detectors

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

2.3.5.2 All motion detectors to be installed at manufacturers recommended height.

2.3.5.3 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.

2.3.5.4 Devices must be ULC approved for commercial use.

2.3.6 Glass Break Detectors/Shock Sensors

2.3.6.1 If approved for use, all devices shall be installed and field-adjusted, tested and commissioned as per manufacturer's specifications.

2.3.6.2 Devices must be ULC approved for commercial use

2.3.7 Door/Window Contacts

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

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

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

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

2.3.7.5 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.

2.3.7.6 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.

2.3.7.7 DPDT contacts are reserved for security systems only

2.3.7.8 Devices must be ULC approved for commercial use.

2.3.8 Monitoring

2.3.8.1 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.

2.3.8.2 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.

2.3.8.3 Where applicable, ethernet cabling to be installed by PHSA and to be dedicated to the alarm system.

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

2.3.9 Ethernet

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

2.3.9.2 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.

2.3.10 Cellular Communication (GSM)

2.3.10.1 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.

2.3.10.2 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.).

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

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

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

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

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

2.3.10.8 Devices must be ULC approved for commercial use.

2.3.11 Intrusion System Programming

2.3.11.1 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.

2.3.11.2 Zone descriptors and naming conventions to be approved by VCH PS.

2.3.11.3 The Health Organization shall supply the Security Integrator with all access codes and IP addresses to be programmed into the alarm system.

2.3.11.4 The panel shall be programmed in SIA format, unless otherwise approved by the Health Organizations.

2.3.11.5 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.

2.3.11.6 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.

2.3.11.7 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.

2.3.11.8 Once the system installation is completed, the Security Integrator shall not access the system either physically or electronically without the Health Organizations' approval.

2.4 Panic/Duress Systems

2.4.1 General

2.4.1.1 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.

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

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

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

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

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

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

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

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

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

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

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

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

2.4.1.14 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).

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

2.4.1.16 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.

2.4.1.17 EOL devices shall be installed at the device.

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

2.4.2 Elevated Risk Areas

2.4.2.1 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.

2.4.3 Devices

2.4.3.1 All hardwired panic/duress buttons must be latching.

2.4.3.2 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".

2.4.4 Monitoring

2.4.4.1 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.

2.4.4.2 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.

2.4.4.3 Where applicable ethernet to be installed by PHSA.

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

2.4.5 Ethernet

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

2.4.5.2 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.

2.4.6 Cellular Communication (GSM)

2.4.6.1 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.

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

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

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

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

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

2.4.6.7 Devices must be ULC approved for commercial use.

2.4.7 Local Response Panic/Duress Systems (Not Monitored)

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

2.4.7.2 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).

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

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

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

2.4.8 Monitored Panic Alarm Systems

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

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

2.4.9 Wireless Panic Alarm Systems

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

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

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

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

2.4.10 Panic / Duress System Programming

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

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

2.4.11 Integration Requirements

2.4.11.1 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.

2.5 Intercom Systems

2.5.1 General

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

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

2.5.1.3 Unless otherwise specified, video intercoms shall be utilized.

2.5.1.4 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.

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

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

2.5.1.7 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.

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

2.5.2 Devices

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

2.5.2.2 Approved manufacturers: Aiphone or approved equivalent.

2.5.3 Intercom System Programming

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

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

2.6 Integration Engine

2.6.1 General

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

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

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

3.0 Appendices

3.1 Appendix 1: Site Specific Requirements – Richmond Hospital (RH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.1.1 Electronic Access Control

3.1.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.1.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.1.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.1.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.1.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.1.2 Closed Circuit Television System (CCTV)

3.1.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.1.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.1.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.
- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.1.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.1.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.1.3 Intrusion Alarm System

3.1.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.1.3.2 Acceptable Manufacturers

- DSC

3.1.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.1.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes Network drop; DLS software.

3.1.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.1.4 Panic/Duress Alarm System

3.1.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.1.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.1.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.1.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.1.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.1.5 Intercom System

3.1.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.1.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.1.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.1.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.1.5.5 Operational Response Communication Method

- Not applicable.

3.2 Appendix 2: Site Specific Requirements – Lion's Gate Hospital (LGH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.2.1 Electronic Access Control

3.2.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.2.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.2.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.2.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.2.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.2.2 Closed Circuit Television System (CCTV)

3.2.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.2.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.2.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.2.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.2.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.2.3 Intrusion Alarm System

3.2.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.2.3.2 Acceptable Manufacturers

- DSC

3.2.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.2.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Network drop; DLS software.

3.2.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.2.4 Panic/Duress Alarm System

3.2.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.2.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.2.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.2.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.2.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.2.5 Intercom System

3.2.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.2.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.2.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.2.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.2.5.5 Operational Response Communication Method

- Not applicable.

3.3 Appendix 3: Site Specific Requirements – Vancouver General Hospital (VGH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.3.1 Electronic Access Control

3.3.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.3.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.3.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.3.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.3.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.3.2 Closed Circuit Television System (CCTV)

3.3.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.3.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.3.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.3.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.3.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.3.3 Intrusion Alarm System

3.3.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.3.3.2 Acceptable Manufacturers

- DSC

3.3.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.3.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Network drop; DLS software.

3.3.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.3.4 Panic/Duress Alarm System

3.3.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.3.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.3.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.3.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.3.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.3.5 Intercom System

3.3.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.3.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.3.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.3.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.3.5.5 Operational Response Communication Method

- Not applicable.

3.4 Appendix 4: Site Specific Requirements – University of British Columbia Hospital (UBCH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.4.1 Electronic Access Control

3.4.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.4.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.4.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.4.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.4.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.4.2 Closed Circuit Television System (CCTV)

3.4.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.4.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.4.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

- Workstation not required unless specifically requested.
- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.4.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.4.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.4.3 Intrusion Alarm System

3.4.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.4.3.2 Acceptable Manufacturers

- DSC

3.4.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.4.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Network drop; DLS software.

3.4.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.4.4 Panic/Duress Alarm System

3.4.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.4.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.4.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.4.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.4.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.4.5 Intercom System

3.4.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.4.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.4.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.4.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.4.5.5 Operational Response Communication Method

- Not applicable.

3.5 Appendix 5: Site Specific Requirements – Squamish General Hospital (SGH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.5.1 Electronic Access Control

3.5.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.5.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.5.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.5.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.5.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.5.2 Closed Circuit Television System (CCTV)

3.5.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.5.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.5.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

- Workstation not required unless specifically requested.
- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.5.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.5.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.5.3 Intrusion Alarm System

3.5.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.5.3.2 Acceptable Manufacturers

- DSC

3.5.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.5.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Network drop; DLS software.

3.5.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.5.4 Panic/Duress Alarm System

3.5.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.5.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.5.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.5.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.5.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.5.5 Intercom System

3.5.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.5.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.5.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.5.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.5.5.5 Operational Response Communication Method

- Not applicable.

3.6 Appendix 6: Site Specific Requirements – Sechelt Hospital (SH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.6.1 Electronic Access Control

3.6.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.6.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.6.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.6.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.6.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.6.2 Closed Circuit Television System (CCTV)

3.6.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.6.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.6.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

- Workstation not required unless specifically requested.
- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.6.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.6.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.6.3 Intrusion Alarm System

3.6.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.6.3.2 Acceptable Manufacturers

- DSC

3.6.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.6.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Network drop; DLS software.

3.6.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.6.4 Panic/Duress Alarm System

3.6.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.6.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.6.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.6.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.6.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.6.5 Intercom System

3.6.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.6.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.6.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.6.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.6.5.5 Operational Response Communication Method

- Not applicable.

3.7 Appendix 7: Site Specific Requirements – qathet General Hospital (qGH)

NOTE: To determine the full scope of system requirements this appendix criteria must be combined with requirements outlined in Sections 1 and 2 of this document.

3.7.1 Electronic Access Control

3.7.1.1 System Overview

- Site wide deployment of card reader system.
- Access cards are combined with photo identification, produced off site.
- Site operation maintained by field panels with main server located off site, connected via Health Organization network.
- CCTV, intrusion and panic/duress are not integrated in to access control system.
- Access control database programming must be completed by the Health Organizations designated Security Integrator. Refer to List of Security Integrators.

3.7.1.2 Acceptable Manufacturer

- Lenel OnGuard PRO

3.7.1.3 Required System Components

- Installation shall include all equipment necessary for full functionality.
- Workstation not required unless specifically requested.

3.7.1.4 Health Organization Supplied Equipment

- System server, network switches.

3.7.1.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.7.2 Closed Circuit Television System (CCTV)

3.7.2.1 System Overview

- Site wide deployment of cameras for security and/or clinical use.

3.7.2.2 Acceptable Manufacturers

- Recording platform: Avigilon.
- Cameras: Avigilon or Health Organization approved equivalent (Avigilon compatible cameras with 100% full feature integration).
- Other components: Avigilon compatible (with 100% feature integration).

3.7.2.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

- Workstation not required unless specifically requested.
- Health Organization supplied equipment includes: Workstation(s), server(s) and network switches.

3.7.2.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Workstation, server(s) and network switches.

3.7.2.5 Operational Response Communication Method

- CCTV system alarms and activities report to site CCTV workstation only.

3.7.3 Intrusion Alarm System

3.7.3.1 System Overview

- Intrusion systems deployed independently throughout campus.
- Systems not integrated into access control or other systems.
- VCH PS requires the ability to program remotely via Health Organizations DLS software.
- Each system to be monitored by Health Organizations' Security Services Contractor. Refer to Alarm Monitoring Section.

3.7.3.2 Acceptable Manufacturers

- DSC

3.7.3.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.7.3.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Network drop; DLS software.

3.7.3.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.7.4 Panic/Duress Alarm System

3.7.4.1 System Overview

- Panic systems deployed independently throughout campus.
- Systems integrated in to DSC for monitoring.

3.7.4.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.7.4.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.7.4.4 Health Organization Supplied Equipment

- Health Organization supplied equipment includes: Telephone line; server for RTLS Systems.

3.7.4.5 Operational Response Communication Method

- Alarms are monitored via contracted ULC monitoring station.

3.7.5 Intercom System

3.7.5.1 System Overview

- Intercoms used on site for basic point to point communication where electronic access control is required.

3.7.5.2 Acceptable Manufacturers

- Refer to Health Organization/ VCH Protection Services for system selection.

3.7.5.3 Required System Components

- Installation shall include all equipment necessary for full functionality.

3.7.5.4 Health Organization Supplied Equipment

- Telephone line, if required.

3.7.5.5 Operational Response Communication Method

- Not applicable.