ELECTRONIC SECURITY SYSTEMS SPECIFICATIONS V 1.5

This document is specific to Interior Health (IH) Hospitals and larger IH facilities and is to be used in conjunction with Division 28 of any project..

UPDATED: MAY 2020

Version Control

The contents of this document cannot be modified without prior written consent from IHA Protection Services

2018-10-25: Version 1.4 Release

- First release of document

2020-5-13: Version 1.5 Release

- Updated release information
  - Changes to back up power requirements
  - Changes to VMS requirements
  - Changes to Card Reader requirements
  - Changes to back up power requirements
  - General format changes

Table of Contents

SECTION 1 – GENERAL REQUIREMENTS

1.1 OVERVIEW OF DOCUMENTS

.1 This document outlines Electronic Security System requirements for Interior Health (IH)

- This document is primarily intended for use at hospitals and/or larger facilities. However, the Protection Services Department oversees Electronic Security Systems within IH 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 Protection Services.

.2 This document outlines the electronic security systems specifications for the following:

- Electronic Access Control Systems
- Video Surveillance systems
- Intrusion Alarm Systems
- Panic Alarm Systems
- Intercom Systems
- Other systems (such as patient wandering/infant protection/staff duress) may interface/integrate with the above noted systems. Where this is required, mandatory input on system design must be sought from clinical users/designates and Protection Services to ensure required functionality is achieved.

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

- Section 1 - General Requirements: outlines requirements that are applicable at all locations of work, generic system requirements, integrators, etc.
- Section 2 – Electronic Security Systems: outlines systems specific information including: Access control; Video Surveillance; Intrusion alarm; Panic, Intercom.

.4 Systems installations are constantly evolving and being updated. Sites which are in transition may require additional consultation. Contact Protection Services for any additional information required.

1.2 RELATED DOCUMENTS

.1 Privacy Guidelines – Freedom of Information and Protection of Privacy Act (FOIPP).
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

.2 Privacy Guidelines for Use of Video Surveillance Technology by Public Bodies
http://www.cio.gov.bc.ca/cio/priv_leg/foippa/guides_forms/video_security.page

.3 IMIT Communications Infrastructure Specifications
https://www.interiorhealth.ca/AboutUs/BusinessCentre/Construction/Documents/IMIT Infrastructure Specification.pdf

.4 IAHSS Security System Design Guidelines (provided upon request)
Z:\IHA Teams\Corporate Protection\EDUCATION AND COMMUNICATIONS\IAHSS Guidelines\IAHSS Design Guidelins (2015).pdf

.5 Staff Safety Guidelines for Healthcare Facility Design Projects
https://www.interiorhealth.ca/AboutUs/BusinessCentre/Construction/Documents/Staff Safety Guidelines for Healthcare Facility Design Projects.pdf

.6 Interior Health Construction Standards and Polices are general requirements of consultants and contractors engaged on Interior Health projects
https://www.interiorhealth.ca/AboutUs/BusinessCentre/Construction/Pages/Policies.aspx

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 Regulations.
- 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 Contractor(s) shall be fully trained and factory certified on all security systems as required by this document. Any/All work on or integration to Lenel must be performed by a technician with at least a Lenel training designation of “Professional” for Access Control, Intrusion and Video.

.2 All equipment shall remain the sole property of IH and the installing company will not retain ownership or control of the system.

.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.

.4 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.

.5 Panels, computers and other devices are not to be locked out (either by a vendor supplied locking device or electronically by password, etc.)

.6 Provide all passwords, including installer, administrator, and the user passwords for all systems.

.7 IH maintains and manages a central “off-site” 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 IH mandatory integrator.

.8 IH maintains and manages a central “off-site” Video Management System (VMS). Any new installations of a Video Surveillance system must integrate and be 100% compatible with the IH Genetec VMS.

.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 IH with 100% integration prior to work commencing by the contractor.

1.5 LICENCES, APPROVALS, PERMITS AND STANDARDS

.1 The contractor shall be responsible for all permits, licenses, inspections and related fees.

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

.3 Plant Services and/or other IH contacts are required to be consulted prior to the commencement of any work.

.4 The contractor and all workers must be provincially licensed and/or meet all requirements outlined by the Ministry of Justice.

.5 Protection Services oversees Electronic Security Systems within IH 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 Protection Services.

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 IH.

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

.4 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

1.7 OPERATIONAL REQUIREMENTS INCLUDING RESPONSE

.1 Electronic security systems installed in the IH 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 8 hours under normal operating conditions. Note: All batteries are to be a minimum of 7 amp hour.

.3 Each system shall have sufficient power supply to operate the system and 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 response from the contracted security service provider on site. Methods for communicating system alarms and notifications vary from site to site. Contact Protection Services department 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 and also meet the IMIT Communications Infrastructure Standards.

.2 All camera installations to be IP/Network based.

.3 All IP/Networked cabling required for Video Surveillance installations **must** follow IMIT Communications Infrastructure Standards and must be installed by an authorized contractor.

.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 Contractor(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 by Protection Services and/or IMIT.

.7 Video Signal Cabling for analogue devices for interconnection between equipment shall be minimum RG-59 type, solid bare copper center conductor with a minimum 95% copper braid shield. For cable runs over 100 meters in length, RG-6 cable may be used. All Video Surveillance coaxial cable connections shall be made using crimped or pre- manufactured connectors only, twist on connectors are not permitted.

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

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

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 The integrator/installer is to provide all hardware, computers, servers, printers and other supporting peripheral equipment as required, unless otherwise stated.

.3. Contractor supplied equipment to meet or exceed IH IMIT and Manufactures requirements, where applicable.

.4 Contractors are required to determine in advance, which equipment will be supplied by Interior Health, and which equipment will be required to be supplied by the contractor.

.5 Where required, software/software licenses and any other required licensing is to be supplied by the installer/integrator unless otherwise stated, including all software required for owners supplied hardware and equipment.

.6 Card Reader/Camera and other device licenses required will be supplied by the integrator/installer for installations. If project scope does not include this requirement, Protection Services must be contacted to verify requirement and number of licenses needed.

Note: If Contractor is not a Lenel VAR on Record with IH, a cash allowance (based on MSRP) for licensing must be carried. Refer to approved mandatory Integrator list for contact information and to obtain costs.

1.10 COORDINATION OF WORK

.1 Installation contractor(s) shall coordinate work with IH and their appointed representatives to ensure systems are installed, programmed, tested, commissioned and verified fully operational to the satisfaction of IH.

.2 IH alarm accounts will be monitored by the identified monitoring and response agency. This includes intrusion, panic and other applicable systems.

.3 Coordination with the Provincial Health Services Authority (PHSA) and/or IMIT may be required for computer, software and peripheral devices (including any wireless components).

.4 Coordinate and cooperate with other trades, including In-house/Facilities staff, for timely completion of all work.

.5 Some or all work may be required to be performed after regular business hours to avoid disruption to the delivery of patient care.

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 The contractor shall test and commission fully operational and functional systems prior to turnover to IH. IH reserves the right to verify the contractor’s test results to determine if system operation is satisfactory and contractor will be responsible to correct any deficiencies at no additional cost to IH.

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

- Cable number
- Source

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

.5 All work shall be installed in a neat and workmanlike manner. The contractor is responsible for cleanup 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 after 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 AHJ and IMIT Communications Infrastructure Standards. Conduits or cables shall be tightly fitted and fire stopped where necessary to maintain fire rating.

.8 Contractor(s) shall repair at no cost to the IH/Owner, 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 within the protected space (i.e. – panels and equipment shall not be mounted in electrical or data rooms that are not within the protected space). Head-end security equipment for Access Control and Video Surveillance shall be mounted at locations designated by Protection Services.

.10 Prior to installation of all panels in communication rooms, final placement to be approved by IH's IMIT Facilities Project Coordinator (IMITFPC) via email to IMITFPC@interiorhealth.ca in order to ensure placement does not interfere with any existing or future planned active telecommunications equipment.

.11 Ground security equipment as per manufacturer's recommendations.

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

.13 All digital inputs are required to have end of line 4 state supervision.

.14 Follow J-STD-607-A-2002 (CSA-527) Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications and the most current version of the CEC.

.15 Unless otherwise specified, IH security systems do not require conduit – except in exposed or exterior locations; however, all wiring shall be concealed unless otherwise authorized by Protection Services.

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

.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 contractor shall coordinate installation of conduit and raceways with electrical contractor to meet these requirements. If using a cable tray as a pathway for cable installation, cabling is to be bundled separately for IH's network cabling.

- Conduit not to be filled past 40% capacity and follow the IMIT Communications Infrastructure Standards for cable colour (green).

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

1.12 PROGRAMMING

.1 All system(s) programming is to be completed by the contractor in consultation with Protection Services.

.2 Cameras are to be set to record (motion only) as soon as the installation will allow, even if network connection to the IH network is not possible at time of install.

.3 All system devices and components are to be programmed to the satisfaction of Protection Services

.4 The contactor is to cover all associated costs of programming.

Note: Lenel Access control and Video Surveillance programming must be completed by a mandatory integrator (refer to Section 1.20.2).If Contractor is not a VAR on Record with IH, a cash allowance (based on MSRP) for this work must be carried.

.5 Protection Services has defined naming conventions that must be used in any Lenel/VMS deployment. The contractor is required to contact Protection Services to ensure that they have the requirements and details needed prior to commissioning the system.

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

1.13 DOCUMENTATION

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

- All user manuals, electronic and/or paper, if required.
- Equipment schedule detailing installation.
- As-built drawings (electronic only, in a suitable format for IH) showing location of all devices, controls, demark connection, panels, keypads, riser diagrams, panel termination details.
    - 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, electronic and/or paper if required.
- Device verification sign-off sheets, electronic and/or paper if required.
- Manufacturer's cut sheets for all devices, electronic and/or paper if required.
- Infection control documentation, if required.
- Documentation outlining the IP schemes utilized in the installation.
- All forms completed as supplied by IH.
- Municipal and other required electrical permits.
- Warranty Certificate, if required.

.2 All documentation to be submitted to IH's designate, as required.

.3 Contractor(s) shall provide IH 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, if required.

1.14 TRAINING

.1 Training shall be provided for each individual system as required by this document. Training shall include a minimum of two (2) hours per individual

system and shall be conducted at a time that is mutually agreeable to both the contractor and the user(s) requiring the training.

1.15 WARRANTY

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

.2 Defective equipment to be repaired at site, and failing this a suitable replacement unit shall be supplied to keep the system operational until the original unit is returned.

1.16 ALARM MONITORING

1.16.1 Overview

.1 IH 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 the Protection Services Electronic Security System Specifications.

.3 Account numbers and other applicable information shall be provided by authorized monitoring agent/station, if applicable, through Protection Services.

.4 If the off-site monitoring company is not identified in the scope of the project the Contractor is to contact Protection Services for direction.

1.17 CONTRACTOR RESPONSIBILITIES

.1 The contractor shall insure that all required information is provided to the monitoring agent/station as required.

.2 The contractor shall complete the user list in conjunction with the user/client (tenant) who will provide details of authorized users. Contractor shall fully program the system accordingly with all required credentials.

.3 The contractor is responsible for any costs associated with off-site monitoring set-up.

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

.5 All passwords for all devices to be supplied to the owner

.6 All information related to installations is considered strictly confidential and the contractor shall guarantee non-disclosure of information.

1.18 CLIENT (TENANT) RESPONSIBILITIES

.1 Once the system is installed and commissioned the user/client (tenant) is responsible to manage the User List function and maintain the database ensuring that all subsequent changes to personnel are noted and reported to monitoring agent/station

1.19 LIST OF INTEGRATORS

.1 Preferred Integrators (alphabetically) for listed systems include:

- Chubb
  Security Systems, Monitoring & Fire Alarm Systems | Chubb Edwards

- Houle Security

https://houle.ca

- Paladin Security
  https://www.paladinsecurity.com

- Terracom
  Terracom Systems | Systems Integration | West Kelowna, Okanagan, British Columbia

.2 Mandatory integrators (alphabetically) required for installation/programming and commissioning/verification of any Lenel access control or integration to Lenel are:

- Chubb
  Security Systems, Monitoring & Fire Alarm Systems | Chubb Edwards

- Houle Security
  https://houle.ca

- Paladin Security
  https://www.paladinsecurity.com

SECTION 2 - ELECTRONIC SECURITY SYSTEMS

2.1 ACCESS CONTROL (CARD READER) SYSTEM

2.1.1 General

.1 Access control systems shall be installed in protected space based on IH/Protection Services 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 Elevator control, where required, shall be installed to allow for control of the elevator on a floor by floor basis.

.3 The system shall be provided with 20% hardware and software spare capacity in addition to installed components. Existing spare capacity shall not be utilized unless approved, in writing, by Protection Services.

.4 The contractor shall provide new hardware and software/licensing for all installations. If existing equipment (i.e. Reader) is already licensed and is being replaced/or moved, then licensing transfer is acceptable.

.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.

.6 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 operations 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.

- The use of Global I/O's is not preferred and must be approved by IH Protection Services prior to installation.

.7 Magnetic locks are not permitted unless authorized by Protection Services. Where authorized, the contractor is required to seek approvals from all authorities having Jurisdiction (i.e. Fire Department) and supply the required permits and/or variance to IH.

.8 All Card reader installations are to be Dual format proximity type able to accept all current IH Gprox and HID card formats**.**

.9 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 by Protection Services.

.10 Lenel Access control database programming must be completed by a mandatory integrator (Refer to Integrator section 1.20.2).

.11 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.1.2 Card Readers

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

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

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

.4 All readers to be installed between 46” to 54” AFF unless directed otherwise.

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

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

.7 Readers shall be black unless otherwise specified

2.1.3 Request to Exit Devices (REX)

.1 Requests to Exit (REX) motion sensor will allow egress through monitored doors without creating alarms with REX connected to bypass door alarm on exit.

.2 Provide acceptable REX devices to meet required functionality. Noting that the use of a REX “button” may be used if a motion sensor does not meet the required needs of the portal/door.

.3 The REX detector 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 Protection Services.

.4 REX 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

.1 Unless otherwise specified, electric strikes or electrified 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. For Magnetic locks refer to section 2.1.1.7

.2 Unless otherwise directed electric strikes and locksets shall fail “**secure**”

.3 Provide additional dry contact output(s) for automatic door operator (ADO) operations, if required.

.4 Provide electrified door hold open devices, and integrate functions in to access control hardware and software, if required.

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

2.1.5 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.

2.1.6 Remote Door Control

.1 Where required, designated doors will have a control switch/switches installed to control door lock and unlock functions. Switch functions to include permanent lock; permanent unlock; momentary unlock regardless of the schedule/state of the door (door schedule is not to override the switch function).

.3 Access control workstations will not be utilized for remote door control unless authorized in writing by Protection Services.

.4 The switch shall be interfaced with the access control / card access systems where applicable.

.3 The switch will be illuminated to indicate and differentiate between all status functions

.4 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.1.7 Access Control System Programming

.1 Lenel Access control programming must be completed by a mandatory integrator (refer to Section 1.20.2).If Contractor is not a VAR on Record with IH, a cash allowance (based on MSRP) for this work must be carried.

.2 Required programming includes, but not limited to, labeling/naming all devices, graphic user interface, and client software/user setup, Access Level assignment and time zones.

.3 Electronic versions of floor plans, if required, to be supplied by IH/Client.

2.2 VIDEO SURVEILLANCE SYSTEM

2.2.1 Video Applications

.1 Video Surveillance systems may be utilized for 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 (i.e.: A specialized clinical sleep laboratory).

2.2.2 Site Security Video Surveillance Systems

.1 Provide an IP Video Surveillance system that is consisting of colour IP Video surveillance cameras that provide High Definition images, colour monitors located as needed, network video recorder complete with software that controls all parameters of each individual camera, frame by frame recording, pre and post alarm recording, motion detection, sequence switching, multiplexing, adjustable frame speeds, and will record all cameras through event driven recording 24-hours per day, 7 days a week in real time.

.2 IH maintains an “Off-site” Genetec Video Management System (VMS) that all new/upgraded Video Surveillance systems must be networked to and have 100% compatibility.

.2 If applicable, IP Video Surveillance system to integrate with access control, wired panic buttons, intercoms and intrusion detection to allow for higher recording rates during alarm conditions.

.3 Video Surveillance 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; i.e. washrooms, change-rooms or other similar spaces.

.4 IP Video Surveillance display and review system to be network-based application allowing for authorized users to remotely view, control and manage all aspects of the IP Video Surveillance system across the network. System will have network and web access for remote monitoring, using predefined user authentication.

.5 Display and review for all the cameras to be accessible through multi-screen workstations located as per Protection Services direction. Contractor is to provide IP Video Surveillance workstations with all required operating and application software, monitors, keyboard, mouse with interconnection to security system network.

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

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

.8 Fire Rated or two coats of CSA approved fire retardant white paint Plywood backing required for wall mount monitor installations.

.9 Exterior enclosures/equipment must be NEMA rated.

.11 Cameras and enclosures used for clinical purposes or in clinical areas must be rated by the manufacturer for use in the specific environment. i.e.: Cameras for seclusion rooms must be anti-ligature and specifically designed for high risk clinical environments.

.12 Cameras and recorder must be configured to accommodate the following:

- Updated default admin account password (to be provided by IH at time of install)
- Disable all ‘audio’ recording abilities on camera / recorder at time of install
- Configure recorder to automatically purge recorder footage after 30 days.
- Configure recorder to be set to appropriate time zone, and configure NTP settings on recorder/cameras/appliance to point to HA specific NTP server

.13 Acceptable manufacturer: required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.2.3 General Clinical Observation Video Surveillance Systems

.1 Clinical Video surveillance systems are to be installed for observation only: recording of camera images is not permitted unless approved in writing by Protection Services.

.2 The Video Surveillance systems shall include all equipment necessary for a fully functioning system.

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

.4 Cameras shall be monitored by an operator. Output must be available for viewing by authorized persons at multiple locations, if required.

.5 Clinical camera systems are not to be connected or integrated into security camera systems in any way unless approved in writing by Protection Services.

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

.7 Outdoor cameras will allow operation in extreme temperatures.

.8 Images to be displayed 24/7 without interruption. For example, screensaver activation is not acceptable; login timeout is not acceptable.

.9 Coax cable installations are acceptable for clinical Video Surveillance systems. If an IP based solution is utilized, the installation is required to be in compliance with IMIT Communications Infrastructure Standards.

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

.11 Video Surveillance systems shall be protected from lightning and power surges.

.12 Exterior enclosures/equipment must be NEMA rated.

.13 Clinical cameras and enclosures must be rated by the manufacturer for use in the specific environment. i.e.: Cameras for seclusion rooms must be anti-ligature and specifically designed for high risk clinical environments.

.14 Required system components and owner supplied equipment is site specific. If not detailed in the project scope, contact Protection Services for requirements and details

2.2.4 Cameras

.1 Provide colour, high-resolution, high sensitivity (day/night) fixed smoke dome type with an auto iris fixed dome cameras with auto-iris lens operation. The mounting is to be appropriate for the environment, unobtrusive and matching colour with hidden cabling. Fixed cameras to be vandal resistant wall mounted and / or mounted at protective locations and heights.

.2 Net new camera installs must be IP/Network cameras. For situations where an Analog camera is better suited, consultation with Protection Services is required. Installation is required to be in compliance with IMIT Communications Infrastructure Standards.

.3 The camera shall be high resolution colour (minimum 2 megapixel (MP) and must automatically switch the camera from colour to black and white mode in extreme low light conditions.

.3 Camera resolutions are to be selected to achieve a minimum of 75 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 dome cameras with 3-9mm lens; greater than 3MP FOV up to 80' length x 45' wide (FOV)

.4 The outdoor camera shall offer protection against the elements that allow operation in extreme temperatures. The camera's operating temperature range shall be -20° to 50° Celsius.

.5 The camera shall operate on 12 or 24VAC, DC or POE, and must automatically detect the applied voltage.

.6 Where IP cameras are installed; all cameras and converters shall integrate 100% with site specific recording platform.

.7 All Cameras must have default password updated during install (provided by Protection Services at the time of install)

.8 Non IP camera connections shall be crimped.

2.2.5 Video Recording System and Storage

.1 Video recording platforms may differ depending on location. Required system components and owner supplied equipment is site specific. If not specified in the project scope the contractor must contact Protection Services for details and requirements.

.2 Provide the appropriate encoding/decoding capability to support 2-way (video and control) communications with any and all IP Video Surveillance cameras, individually and/or in predetermined clusters via the security Ethernet infrastructure.

.3 The system shall be able to record clear images of individuals, which is to allow distinction of gender, ethnicity and age category. The system is to provide recorded images of sufficient quality to be used as court evidence in Canada.

.4 Provide video storage capacities for minimum of 30 days at (30) thirty frames per second, minimum 1080p resolution. Provide all required archive servers with required storage and client workstations. System to have the ability to choose recording rates and quality for each camera, have activity detection and incorporate smart search capabilities. Motion only recording is acceptable. Data retention/storage to be supplied based on:

- H.264 Encoding
- 3MP resolution
- 15 FPS
- 70% Motion
- 30 Days retention
- Full capacity of the appliance (not the camera count at the time of installation)
- Data storage days to be calculated utilizing RAID 6.

.5 Devices to be mounted in a secure location as directed by IMIT and Protection Services. Contractor shall coordinate final mounting location at site prior to installation. Prior to installation of all panels in communication rooms, final placement to be approved by the IH's IMIT Facilities Project Coordinator (IMITFPC) via email to IMITFPC@interiorhealth.ca in order to ensure placement does not interfere with any existing or future planned active telecommunications equipment.

.6 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.2.6 Monitors

.1 Monitors shall be wall or desk mounted as per the project scope or Protection Services.

.2 All monitors shall be high resolution, TFT active matrix LCD monitors, with multimode functionality, minimum 920 x 1080 resolution – minimum 24".

2.2.7 Video Surveillance System Programming

.1 Video Surveillance programming must be completed by a mandatory integrator (refer to Section 1.20.2).If Contractor is not a VAR on Record with IH, a cash allowance (based on MSRP) for this work must be carried.

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

.3 Electronic versions of floor plans, if required, will be supplied by IH.

2.3 INTRUSION ALARM SYSTEM

2.3.1 General

.1 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 The intrusion alarm system must integrate into the Lenel access control system (if applicable), allowing users to be programming in the alarm system using Lenel On guard.

.3 Lenel integration (if applicable) to the alarm panel is required to allow authorized users to arm and disarm using their existing access card + PIN code (if required).

.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 Protection Services.

.6 Modules for GSM and/or IP communication must be supplied to ensure connection if the system is externally monitored.

.7 When partitioned, each partition of the intrusion alarm system will have as a minimum the following devices:

- Full LCD keypad
- Siren

.8 The panel shall be non-proprietary (i.e. available to all alarm contractors).

.9 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).

.10 Battery backup shall be gel-cell type, minimum 7 Amp/Hour. Battery installation date shall be marked on the battery and panel cover.

.11 System panel boxes shall be supervised with tamper switches; end of line (EOL) resistors to be used and require 4 state supervision

.12 EOL devices shall be installed at the device – not in the panel.

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

.14 Fire Rated or two coats of CSA approved fire retardant white paint Plywood backing required for wall mount monitor installations.

.15 Installations include 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.

.16 Provide sirens in the protected space, to alert staff of an alarm condition

.17 Where applicable, devices must be ULC approved for commercial use

.18 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.3.2 Keypads and Panels

.1 All keypads shall be LCD alpha (full English) type.

.2 All keypad panic buttons shall be disabled.

.3 All keypads to be set up for “Quick Arming” (* 0).

.4 All keypads to be installed at 54” AFF

.5 Panel mounting height, should be between 48” AFF to maximum of 96” AFF.

.6 All keypads and panels to be securely fastened to walls with 3/4in trade size, A-C plywood backing capable of supporting attached equipment, including weight of battery as required.

.7 Proper grounding as per manufacturer’s specification.

.8 All panels to be screwed closed.

.9 All panels to be installed within protected space, unless approved in writing by Protection Services.

.10 Acceptable manufacturers: Bosch or approved equivalent.

.11 Prior to installation of all panels in communication rooms, final placement to be approved by IH’s IMIT Facilities Project Coordinator (IMITFPC) via email to IMITFPC@interiorhealth.ca in order to ensure placement does not interfere with any existing or future planned active telecommunications equipment.

2.3.3 Sirens/Strobes

.1 The system shall include sufficient interior alarm siren to provide an audible alarm warning throughout the protected space; more than one siren may be needed to meet this requirement.

.2 Sirens to be a minimum of 100 decibels and not to exceed 120 decibels.

.3 All field devices to be calculated and sized by the contractor and an additional 20% capacity to be supplied.

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

.5 An exterior strobe (blue), where required, shall be installed for all systems, location to be decided 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).

.6 Strobe shall be latched so that the panel must be reset to turn it off. The strobe will provide staff with a warning that the alarm system has been activated.

.7 An audible warning shall be provided when the system is armed or during the exit delay period. The armed warning tone shall be different from the alarm siren sound and shall be audible throughout the protected space. Additional sirens or tone devices to be located throughout the protected space so that all staff can hear the alert.

2.3.4 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.

2.3.5 Glass Break Devices

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

.2 Devices must be ULC approved for commercial use.

2.3.6 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 Devices must be ULC approved for commercial use.

2.3.7 Cellemetry Back-Up

.1 Cellemetry shall be used as a backup method for monitoring only unless approved in writing by Protection Services.

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

.2 The cellemetry power supply shall be hard wired to a dedicated, non- switched circuit (i.e. no plug-in type transformers) and the circuit # clearly identified on both the electrical panel directory and on the alarm panel.

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

.4 The cellemetry panel shall monitor Burglary (a separate zone coded as such) and TLM (telephone line monitoring). These zones shall be coded and identified as coming from the cellemetry panel.

.5 Devices must be ULC approved for commercial use.

2.3.8 Intrusion System Programming

.1 The contractor shall be responsible for all programming of the alarm system. This includes all user codes; all zone definitions and establishing a connection to IH's monitoring station choice.

- The use of 3rd Party Monitoring and/or direct notification via the Lenel and other site notification systems will be site/project specific. It is the contractor's responsibility to ensure alarm notification is designed and programmed as per site/project requirements.

.2 IH/Client/Tenant shall supply the contractor with all access codes and phone numbers to be programmed into the alarm system.

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

.4 The contractor shall program the following:

- Daily test transmission (after 00:01 – 05:00, but not on the hour).
- Bell time-out shall be set at 4 minutes.
- Home-away enabled only if requested by owner
- Opening and closing times.
- Remote download access enabled.
- Access & panel upload codes left at default.
- Unless installer and master codes are supplied by IH/Client/Tenant, the installer and master codes are to be left at default.

.5 The contractor shall not install a contractor's lockout enable and shall not program Forced Arming or Auto-Disarming without prior approval from Protection Services.

.6 Upon completion of programming the installer shall initiate an upload of the panel programming to IH's authorized monitoring agent.

.7 Once the system installation is complete, the contractor shall not access the system either physically or electronically without IH approval.

2.3.9 Intrusion System Monitoring (Intrusion/Panic/Duress)

.1 IH retains the right to monitor their alarm systems in the manner of their choice and will not be locked into any other monitoring arrangements as a result of alarm system installations.

.2 Contractor shall provide telephone connectivity (hardware & software) to IH's authorized monitoring agent/station in order to facilitate a security response. Costs for setup and coordination, if applicable, are the responsibility of the contractor.

.3 Where applicable, telephone lines to be installed by Telus in coordination with IH IMIT. Telephone line to be dedicated to the alarm system and telephone line

used for monitoring is not to be shared with other devices (the contractor is not permitted to utilize existing fax lines for monitoring).

.4 All telephone jacks used for alarm/security systems shall be wired to USOC RJ45 industry standards. All position eight (8) jacks shall be installed with a tamper loop, ahead of the demark block.

.5 Alarm panels are to be programmed for remote administration by IH and the security response company as identified.

2.4 PUBLIC PANIC AND STAFF DURESS SYSTEMS (WIRED)

2.4.1 General

.1 The Panic/Duress buttons shall utilize self-diagnostic, self-monitoring and reporting technology.

.2 The Panic/Duress systems, if required, are to be integrated to other security systems (access control, video surveillance and Radio system) either directly or via integration to allow for all panic alarms to be displayed/monitored/announced at locations identified in the project scope.

.3 Upon activation of any panic/duress button, the exact unit ID and location are to be annunciated to the mapping software and, if applicable, the Radio system and the staff workstation locations.

.4 All fixed buttons to be mounted at 48” to 56” AFF unless otherwise noted with protective covers.

.5 System panel boxes shall be supervised with tamper switches; end of line (EOL) resistors to be used and require 4 state supervision.

.6 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.4.2 Devices

.1 Panic/Duress buttons are to be hard wired with a lit (Red) mushroom style button and key reset. The buttons shall be equipped with strobe light and annunciation after the alarm activation.

.2 Exterior buttons (Parking lot and underground parking) to be wall mounted or pole mounted in well-lit areas spaced such that no spot may be more than a maximum of 30m from a panic button, maximum of 10m from the parking area edge, and at all parking area entrances.

.3 Interior buttons to be strategically wall mounted, suitably sized and identified/clearly labelled for “security emergency.”

.4 Acceptable manufacturers: Under counter buttons: HUB; Wall buttons: STI Model SS2221 with custom features including audible alert and cover.

2.4.3 Non-Monitored Panic Alarm (local response)

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

.2 The system is to inter-connect to intrusion alarm system and separately report panic/duress alarms through the system and, if applicable, to the Security 2-way radios, pagers and alarm system (“map pods”) in the security office to allow

security monitoring staff to individually identify the location point and origin of the alarm.

.3 The contractor is responsible to ensure that the sequence of events and notifications following an activation of the system is per Protection Services requirements.

- The annunciation process and devices will differ from Site to Site. Protection Services will provide the information upon request.

.4 The panic/duress alarm panel will be controlled by an LED keypad that will clearly identify the location of each panic button.

.5 If more than 16 panic buttons are required then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panels.

.6 Make and model of panic button shall be decided in consultation with Protection Services.

.7 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.4.4 Monitored Panic Alarm (external response)

.1 As per above specifications, except that each panic button shall be connected to the main intrusion alarm system panel and each panic button shall be identified as an individual zone. If more than 16 panic buttons are required then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panel(s).

.2 Protection Services and/or the client is to be consulted as to whether or not monitored panic/duress buttons will also report locally. (Note that most monitored panic alarms do not report locally - either audibly or with a strobe).

.3 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.4.5 Panic System Programming

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

.2 Electronic versions of floor plans, if required, to be supplied by IH.

2.5 STAFF DURESS SYSTEM (WIRELESS)

2.5.1 General

.1 Staff Duress systems can utilize either an RTLS solution or an Intrusion Alarm system.

- If via RTLS:
  - It shall be server-based and allow any Authority connected workstations to access the system for supervision, mapping and reporting purposes. Dedicated wall-mounted monitors and workstations shall be placed in all Care Team Stations where the system is required.
  - The system cannot utilise an 802.11 wireless network or the IH network.

    - If applicable, the system shall be fully integrated with the nurse call system on a room-by-room basis, such that alarms actuate the zone light for the departmental wing as well as the dome light above the room door, and annunciate the location at the nearest nurse call console. Via the nurse call system, staff duress alarms stating location shall also be annunciated through staff communication system (Vocera).
- If via Intrusion Alarm:
    - Duress buttons shall utilize self-diagnostic, self-monitoring and reporting technology.
    - Duress systems, if required, are to be integrated to other security systems (access control, video surveillance) either directly or via integration to allow for all alarms to be displayed/monitored and announced at locations identified in the project scope.
    - Upon activation of any duress button, the exact unit ID and location are to be annunciated to the mapping software and, if applicable, the staff workstation locations.

.2 A complete structured cabling infrastructure is to be installed to allow a complete system network, including receivers, repeaters and exciters.

.3 System panel boxes shall be supervised with tamper switches; end of line (EOL) resistors to be used and require 4 state supervision.

.4 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.5.2 Devices

.1 All wireless buttons/badges must have replaceable batteries.

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

.3 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.5.3 Non-Monitored Duress Alarm (with local response)

.1 Where specified, install a local response duress system which is not externally monitored for a response.

.2 Local duress systems will not be integrated into the main intrusion alarm panel (if monitored) unless specified by Protection Services.

.3 The contractor is responsible to ensure that the sequence of events and notifications following an activation of the system is per Protection Services requirements.

    - The annunciation process and devices will differ from Site to Site. Protection Services will provide the information upon request.

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

.5 Each standalone panic alarm panel will be controlled by an LED keypad that will clearly identify the location of each panic button.

.6 If more than 16 panic buttons are required then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panels.

.7 Make and model of panic button shall be decided in consultation with Protection Services.

.8 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.5.4 Monitored Duress Alarm (external response)

.1 As per above specifications, except that each panic button shall be connected to the main intrusion alarm system panel and each panic button shall be identified as an individual zone. If more than 16 panic buttons are required then the panic alarm system shall annunciate to appropriately sized LED graphic annunciator panel(s).

.2 Protection Services and/or the client is to be consulted as to whether or not monitored panic buttons will also report locally. (Note that most monitored panic alarms do not report locally - either audibly or with a strobe).

.3 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.5.5 Duress Alarm System Programming

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

.2 Electronic versions of floor plans, if required, to be supplied by IH.

2.6 INTERCOM SYSTEMS

2.6.1 General

.1 Where required, intercom(s) systems will be installed for communications.

.2 Unless otherwise specified, video intercoms will be utilized

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

.4 Point to point / hard wired intercom(s) to be used unless otherwise specified

.5 PBX/telephone system based intercom(s) may be utilized in certain conditions and must be approved, in writing by the IMIT and Protection Services

.6 Acceptable manufacturer, required system components and owner supplied equipment may be site specific. If not detailed in project scope, contact Protection Services for details and requirements.

2.6.2 Devices

.1 Intercom cameras to be minimum 180 degree field of view (FOV)

.2 Approved manufacturers: A-phone or approved equivalent

2.6.3 Intercom System Programming

.1 Program the system and associated components to the satisfaction of the owner.

.2 Required programming includes, but not limited to, labeling/naming all devices, graphic user interface, and client software/user setup. Some deployment applications may require programming to the electronic access control system.