The Regional Municipality of Durham

Works Department

Facilities Maintenance and Operations

Security Services Installation and Security Systems Standards

Version 3.14 – Mar 11th, 2024

Table of Contents

1 Purpose

To provide a detailed guideline for the installation of security systems and a set of standards for the equipment to be used in the installation of security systems at regional facilities.

2 Technical Abbreviations

AC	Alternating Current
AMP	Ampere
CAD	Computer Aided Drawing
CCTV	Closed Circuit Television
CRI	Color Rendering Index
DVR	Digital Video Recorder
EOL	End of Line
GSM	Global System for Mobile
HSCIP	High Security Communication Internet Protocol
IP	Internet Protocol
LCD	Liquid Crystal Display
MAC	Media Access Control
NAR	Nuisance Alarm Rates
NC	Normally Closed
NO	Normally Open
PD	Probability of Detection
PPS	Physical Protection System

PSS	Physical Security System
SMTP	Simple Mail Transfer Protocol
UPS	Uninterruptable Power Supply
WAN	Wide Area Network

3 General Guidelines

3.1 Product Selection

Where products are not specified, proposed products must be confirmed with Security Services for suitability and compatibility prior to procurement. Proposed products should be high quality, industry standards with a proven track record of reliability and be quickly and easily obtainable from multiple sources to reduce downtime in the event repairs. They need to minimize nuisance alarm rates (NAR) while maintaining a high probability of detection (PD). Any quality manufacturer should have PD and NAR rates readily available for all their sensor products.

3.2 Existing Security System

Any addition or renovation to a facility that has a pre-existing security system needs to ensure compatibility and tie-in with the existing system. If the existing system is not compatible due to the age of the system, upgrading of the existing system needs to be coordinated with the new project.

3.3 Cabling

Controllers and devices should be wired neatly. Cables should have enough slack to allow for restriping and terminating the cables in the event of hardware changes while not leaving so much slack as to overburden the enclosure. Cables should be run at 90 degrees with an appropriate amount of cable tie-down points. Care should be taken to not “drape” cables across control boards.

Cable run through ceilings should be in conduit or in a cable tray. If that is not possible, then the cable must be plenum-rated and suspended so it does not lie on the ceiling. The method of suspension cannot affect the ability to pull new cable (i.e., “J” hooks are acceptable; tie-wrapping cable to drop ceiling support wires is not).

All cabling at panel locations is required to be labelled with a label maker. Name of device with corresponding drawing door / room number (Door 345 ES, Room 175 Motion, etc.)

All devices should be installed and wired as per manufacturer's specification. All cable should be supplied, installed, and terminated according to manufacturer's specification.

Any cable run through a new, or existing, fire separation must be sealed as per current fire code.

Cable run outside of the data room needs to be protected from tampering using metal conduit, PVC conduit, cable armoring, etc.

Cabling within the cabinet should be installed in slotted wire finger duct (1" Width x 2" Height)

Cabling standard for security devices.

Wiegand Readers – 22/10 Conductor FT6 Shielded

RS-485 Readers - 24/4 Conductor FT6 Shielded twisted. (Purple or approved colour by security services)

Motion, glass breaks, request to exit motions and buttons, panic buttons, door release buttons, and Door contacts – 22/4 Conductor FT6

Strikes – 18/2 Conductor FT6

Network – Cat6E FT6 (red)

Communications – 24/4 Conductor FT6 Shielded twisted. (Purple or approved colour by security services)

Underground burial cable to be installed when any cabling is to be run in PVC conduit underground. Cable to follow manufacturing requirements.

Cable length for devices need to meet all manufacture specifications and guidelines.

3.4 Hardware

All ICT equipment must be installed within factory ICT enclosures. All enclosures containing major components should have all components labeled. The label should contain the type of equipment, serial number, and zone range, if applicable. The label should be made of laminated plastic 1/8” thick, white with a black center core. They should be a minimum of 1” X 3” with minimum ¼” high engraved block lettering.

3.5 Ladders

Access ladders should be enclosed below 12 feet to prevent climbing by unauthorized personal. Ladder covers should be monitored with contacts to notify regional staff in the event of unauthorized access. Care should be taken to not run other services near the ladder to prevent individuals from bypassing the enclosure.

3.6 Door Hardware

Door hardware appropriate for the specific environment must be used. This is especially important in areas where the hardware will be exposed to chemicals that will accelerate the corrosion process.

3.7 Network Connection

Any device that will be connected to the Region of Durham network needs to be coordinated well in advance with Corporate Services – Information Technology (CS-IT). Typically, they require **30 days’ notice**, need media access control (MAC) addresses for all the hardware to be installed on site and will provide the range of IP addresses to be used.

3.8 Work Safe Practice

All work should be done in a safe manner in accordance with all jurisdictional authorities and any additional site-specific requirements.

3.9 Warranty

The warranty period for all items shall be minimum 2 years, inclusive of parts and labour.

4 Access Control and Intrusion System

4.1 Power

All AC power should be hard-wired on a dedicated 15 Amp circuit, no additional cord and plug connected device(s) should be allowed.

Backup batteries must be installed for all ICT power supplies. Batteries must be 12v 7ah batteries and be labeled with the month and year of installation.

All ICT equipment and security devices must be powered from the ICT power supplies in cabinets.

When installing modules like CX-12, CX-33, wireless panic modules, wireless receiver, security voice paging system, and LED strobes. They must be powered by a ICT power supply with battery backup.

All Locking devices must be powered from ICT power supplies.

All Maglock must be powered from Maglock power supplies.

4.2 Security System

The Region of Durham has standardized on the ICT Integrated Access Control and Intrusion Platform running on Protégé GX software.

The security integrator must be a certified installer and authorized dealer for ICT and be able to purchase equipment from ICT directly. Proof of ICT certification must be provided prior to award of a contract/job.

The security integrator will be responsible for testing the complete system on site using test users. Once the local testing is complete the security integrator will supply a complete system configuration file (in Excel spreadsheet or similar format) to Security Services, who will program the site in the regional server. The Integrator will provide all required maps to configure the active map feature for site control.

The main control panel must be an ICT PRT-CTRL-DIN panel with a PRT-PSU-DIN-2A power supply running the most recent ICT firmware version.

For connection back to regional headquarters for programming a network connection is required. Where no WAN is available a Cisco cellular router should be installed to facilitate the connection. These routers can be ordered through the Region of Durham procurement contracts. Telephony and CS-IT will need to be involved to properly setup the device prior to installation on site.

Mounting of wireless router should be wall mounted according to manufacture installation guidelines as well as to optimize the best signal within a facility.

The integrator will be responsible for the coordination and activation of a new monitoring account, with the Regions monitoring account provider where one does not exist. Any costs associated with the account activation will be carried by the integrator.

If the site is to be monitored for alarms, a global system for mobile (GSM) unit needs to be installed for backup communications. The current GSM unit is model #DSC LE4000 with appropriate antenna kit to ensure optimal signal strength, a newer model should be installed if available. The unit will be specified if it needs to be Rogers or Bell compatible to ensure it is redundant to the main communication provider to site.

GSM mounting height should be at least 7 feet where possible and optimize best signal within a facility.

4.3 Door Controllers, Modules, Readers, and Keypads

Access control doors will use ICT door controllers in appropriately sized enclosures with hard-wired power, running the latest ICT firmware.

Point expansion modules will be appropriately sized ICT modules running the most recent ICT firmware.

Sites that require elevator floor control must use the ICT elevator interface modules in an appropriately sized enclosure running the most recent firmware.

Card readers will be ICT V3 (or newer model that is compatible to our platform) multi-function high security readers. They can be switch-plate or mullion mount, standard reader or arming station (keypad equipped). Once installed readers will be programmed/flashed to remain red when door is locked and green when unlocked. Where required an ICT back box for the mullion or single gang reader will be installed (either on block wall or metal surfaces). All installations will require a ferrite back plate. All new ICT readers are required to be wired RS-485.

LCD Keypads will be ICT Keypads. Locations that are not staffed or industrial setting a Protégé Alphanumeric LCD Keypad should be used (Part # PRT-KLCD). Locations that are in an office setting and staffed regularly a Protégé Touch Sense LCD Keypad – Black should be used (Part # PRT-KLCS-B). Security Services staff can advise what and where we deem these products to be deployed prior to installation.

All Controllers, modules, readers, keypads, and all other ICT equipment can not be company propriety ICT equipment in any way. This includes and is not limited to sticker, logos, stamps, firmware, software, device naming, branding, etc.

All firmware uploaded for any ICT modules or devices must be available from the ICT official website and must not be beta version firmware.

4.4 Contacts and Motion Detection

Concealed door contacts should be 1” diameter 3-wire, capable of being wired as normally closed (NC) or normally open (NO) with an end of line (EOL) resistor. It should be installed in the field NC with the 2x 1k EOL resistor at the device. Gap distance in a steel frame should be no more than ½” and in a wooden frame, no more than 1”. In a steel door with a recessed trough on the top edge, it is acceptable to use a rare earth magnet in compression housing. If the door has access control, the contact should be wired back to the door controller.

Surface contacts should be capable of being wired as NC or NO with an EOL resistor. It should be installed in the field NC with the 2x 1k EOL resistor at the device. Gap distance should be no more than ¾”.

Overhead door contacts should be capable of being wired as NC or NO with an EOL resistor. It should be installed in the field NC with the 2x 1k EOL resistor at the device. Gap distance should be between 2” and 6”. They must be installed as a rail mount style mount contact 6 to 12 inches off the floor. The tail/wire lead on the overhead door contact must be armored.

Motion detectors should be dual tech at a minimum, using passive infra-red and microwave detection. The sensors should have the pet immunity and tamper detection functions available. They should be able to be wired NC or NO/EOL. It should be installed in the field NC with the 2x 1k EOL with the resister at the device and running through the tamper loop. Care should be taken when selecting the mounting location to reduce the risk of false alarm from heat sources and optimize device performance in accordance to manufacture guidelines.

Glass break detectors should have sensitivity adjustments to account for room acoustics and be adequate for the area to be covered. They should be able to be wired NC or NO/EOL and have tamper detection. It should be installed in the field NC with the 2x 1k EOL with the resister at the device and running through the tamper loop.

4.5 Door Strikes and Locks

Electric door strikes (mortise or RIM type) should be fail-secure by default. Fail-safe strikes should only be used where they are placed in an evacuation route which requires the door to be swung in. If the door swings out, a fail-secure strike shall be used with free egress door hardware. If a fail-safe device is used it must not be hooked up to backup battery power and should have a current limiting device to reduce heat. They should operate on 12V DC power. In-rush current should not exceed one ampere (1A) and holding current should not exceed 500 milliampere (mA). The actuating solenoid should move from the fully secure position to the fully open position in not more than 500 milliseconds (ms). The strike selected should be appropriate for the size and weight of the door and the mechanism should be encased in a hardened guard barrier to deter forced entry.

All electric strikes (mortise and rim type) will require the installation of a diode at the end of line at the strike location. Diodes are also required when using the integration of a Camden door operating device (cx-12 plus, Cx-33, etc.)

Electromagnetic locks should be avoided where possible. If required for a specific application, it should contain no moving parts and generate at least 1,200 lbs. (544 kg) of holding force. It must release in the event of a power failure or fire-alarm and should have no back-up power. It should operate on 12 VDC power and contain internal circuitry to eliminate residual magnetism and inductive kickback. It should not dissipate more than 12 watts and the holding current should be no greater than 500 mA. It should go from the fully secure to fully released state in no greater than 300ms. The electromagnetic locking mechanism should be encased in a hardened guard barrier to deter forced entry. Installation shall follow the local jurisdiction having authority.

4.6 Panic/Holdup Devices

Bell or Alarm boxes should be mounted in a highly visible area high enough to be out of easy reach. The enclosure should be monitored for tampering with a supervised tamper switch.

Panic/Holdup buttons should be Potter momentary buttons (part # HUB-M) wired NC with the 2x 1k EOL resistor at the device.

Door release buttons should be RCI rocker switches (part # 909S-MO) wired NC with the 2x 1k EOL resistor at the device.

Automatic request to exit devices should be motion activated with adjustable detection area, adjustable sensitivity and built in LED indicators. It should have tamper protection, run on 12 VDC and have an adjustable relay timer. The device should be wired NC with the 2x 1k EOL resistor at the device.

Wireless panic/holdup receivers should be Inovonics (part # EN4216MR). When installed the device should be wired to monitor low battery and tamper alarms.

Wireless panic/holdup pendants should be Inovonics (part # EN1223S).

This is by no means a complete list of all possible devices but covers standard installation products. Specialized products or applications need to be reviewed on a case-by-case basis.

5 Video Surveillance System

5.1 General

The Region of Durham uses the Digital Watchdog Spectrum Video Management System (VMS), which is a scalable system. The camera load at a specific facility will determine the type and size of recording and control hardware.

All network cable used for the video surveillance system must to be RED Cat6E FT6 cable labeled at both ends. All connectors should have flexible rubber boots. Excess cable at the head end should be kept to a minimum, with enough cable left for routing and re-terminating if necessary. Coils of spare cable should not be left behind unless specifically requested.

All video network connections should terminate on dedicated patch panels and patch to the CCTV network switch. Switch should be D-Link DGS-1210-28MP (or most recent model and firmware).

The uninterruptable power supply (UPS) installed should be capable of handling the load from the switches and NVR for a period of no less than 30 minutes. The UPS needs to be able to transmit simple mail transfer protocol (SMTP) notification from its own on-board network interface card and be able to have its batteries services while in operation. UPS shall be an Xtreme Power P80 1500VA model with optional simple network management protocol (SNMP) notification card (or most recent model).

5.2 Equipment

Head-end equipment (NVR, Switches, UPS, Local Monitors, etc.) should be housed in an appropriately sized lockable rack with proper venting including an inlet (with filter) and outlet fans with temperature sensing capabilities and constant on feature.

All devices shall be programmed with usernames and passwords supplied by the Security Services department. No devices shall have default login and passwords left enabled.

The system will need to record all cameras 24 hours per day, at 10 frames per second for 30 days. The system will also need to handle an additional 50% camera load for future expansion, no system should be installed running at maximum capacity.

1. **Additional Server Requirements (For large scale sites where more than 16 cameras will be installed)**

    - Rack Mount
    - Windows 10 Pro or greater
    - 250 GB SSD Raid Redundant Operating System Drive
    - Intel 7 Processor or greater
    - 16 GB (RAM) Memory or greater
    - 2X Gigabit ethernet ports
    - 600 Mbps video recording rate or greater
    - Video Outputs – HDMI and DVI

2. **Server/Computer Requirements (For sites that have less than 16 cameras installed)**

    - Intel i7-10700 (16 MB cache, 8 cores, 16 threads, 2.90 to 4.80 GHz Turbo, 65W) or greater
    - Windows 10 Pro or greater (Windows 11 Pro)
    - Ram of 32 GB, 2 x 16 GB, DDR4 or greater
    - Internal Hard drive of 512 GB, M.2 2230, PCIe NVMe, SSD, Class 35
    - Additional 3.5 inch HDD Slot internal on PC that will accept minimum 8 TB's of a Surveillance drive
    - Video Outputs of HDMI and DVI
    - Peripheral devices to be included (Mouse, Keyboard) and necessary cables to be connected to monitor and power source

5.3 Cameras

1. Spot monitors required for up to 16 cameras to be displayed should use the Senstar Thin Clint 10D or equivalent. If more than 16 cameras need to be displayed on a spot monitor an independent client computer should be used.

2. Standard interior fixed view camera should be AXIS P3267-LV (or most current version), or equivalent running the most recent firmware.

3. Standard exterior fixed camera should be AXIS P3267-LVE (or most current version), or equivalent running the most recent firmware.

4. Standard long-range exterior fixed camera should be AXIS Q1786-LE (or most current version), or approved equivalent running the most recent firmware.

5. Standard 180° fisheye camera should be AXIS P3818-PVE (or most recent version), or equivalent running the most recent firmware.

6. Standard PTZ camera should be AXIS Q6135-LE (or most recent version), or equivalent running the most recent firmware.

7. Standard 360° camera should be AXIS P3737-PLE (or most recent version), or equivalent running the most recent firmware.

8. Corner mount cameras for elevators/small rooms should be AXIS P9106-V for interior, for harsh environments the AXIS Q9216-SLV should be used.

9. Camera Licensing – Single DW Spectrum IPVMS License – Digital Watchdog Licenses to be provided (Part # DW-SPECTRUMLSC001)

10. VMS – Digital Watchdog 5.0 or latest production version

11. Camera heights for exterior cameras will be 8 – 10 feet from the finished base. This will be determined by manufacturer guidelines and environmental factors (i.e. landscaping) or purpose of camera field of view. For interior they will be mounted with appropriate housing hardware considering heights and purpose of the camera coverage. These items will be discussed prior to installation with a Region Security member once drawings are presented to the Security Department in conjunction with the Region's Project Manager/General Contractor.

Mounting hardware for all exterior cameras needs to be sized appropriately to account for maximum wind and ice loads expected at the site.

Cameras should be configured with appropriate annotations. The NVR should be configured with required cameras layouts and any required camera tours.

All cameras should be properly focused and aimed to provide required views.

6 High Security Locks & Keys

The Region of Durham uses the Mul-T-Lock 3-in-1 high security lock system and owns its own patented keyway. The constructor can use one of our authorized lock installers to perform the work or their own certified Mul-T-Lock installer. If they are going to use their own installer the lock and key order has to be authorized by the Security Services Department before Mul-T-Lock will release the product.

The consultant or project manager will provide layout drawings and door hardware schedules to the Security Services Department who will determine the lock coding for each door and keys required (2 per cylinder). An e-mail will be sent to the locksmith and Mul-T-Lock representative, authorizing release of the indicated products.

Once the locksmith receives the keys and hardware, the products will be turned over to Security Services for distribution prior to scheduling the lock installation.

Offices should be keyed to the Region's standard Schlage office key system.

If a high-security key cabinet is required it shall be the Morse Watchman's KeyWatcher Touch system with card reader access control, large cabinet enclosure with enough internal key control modules.

7 Timelines for System Integration and Programming

High security locks and keys from Mul-T-Lock take an average of 8 weeks to arrive once the order has been authorized. Additional distribution and programming of the key database means these items should be **ordered at least 3 months prior to occupancy**.

The security system configuration files from the integrator should be received by Security Services no less than **30 days prior to occupancy** for programming.

Information required for monitoring, including special alarm response instructions and call lists need to be provided to Security Services **no less than 14 days prior to occupancy**.

Network devices need to be active and correctly programmed on site for Security Services to program the systems. Delays due to coordination issues with CS-IT will result in the system not being functional.

8 Project Close-Out

Camera views and all security system components must be confirmed by Security Services during project close out. The warranty period for any installed items shall not commence until Security Services has signed the Security Services Installation Checklist which will be provided to necessary stakeholders, acknowledging security system functionality. This will be provided once a tender is awarded as it will be tailored to the specifics being installed.

9 Inquiries

For further information regarding this guideline, contact Security Services.

10 Release Notes

- October 10, 2023 – Section 4.2 Integrator must be ICT certified and an authorized dealer for equipment procurement.
- October 23, 2023.
- End of Line Resistors defined in more detail for Intrusion/Access Devices
- Cabling within the cabinet should be installed in slotted wire finger duct (1” W x 2” H)
- Cabling standard for security devices.
- Readers – 22/10 Conductor FT6 Shielded
- Motion, glass breaks, request to exit motions and buttons, panic buttons, door release buttons, and Door contacts – 22/4 Conductor FT6
- Strikes – 18/2 Conductor FT6
- Network – Cat6E FT6 (red)
- Communications – 24/4 Conductor FT6 Shielded twisted. (Purple or approved colour by security services)
- Underground burial cable to be installed when any cabling is to be run in PVC conduit underground. Cable to follow manufacturing requirements.

- Cable length for devices need to meet all manufacture specifications and guidelines.

- December 5, 2023 – section 4.2 installation of cell router/gsm and ICT proof of certification prior to award of bid/job

- January 11th – Section 4.3 – Door Controller, Modules, Readers, and Keypads

  All Controllers, modules, readers, keypads, and all other ICT equipment cannot be company propriety ICT equipment in any way. This includes and is not limited to sticker, logos, stamps, firmware, software, device naming, branding, etc.

  All firmware uploaded for any ICT modules or devices must be available from the ICT official website and must not be beta version firmware.

- Mar 11th, 2024

- Section 3.3 - All cabling at panel locations is required to be labelled with a label maker. Name of device with corresponding drawing door / room number (Door 345 ES, Room 175 Motion, etc.)

- Section 3.3 - Wiegand Readers – 22/10 Conductor FT6 Shielded

- Section 3.3 - RS-485 Readers - 24/4 Conductor FT6 Shielded twisted. (Purple or approved colour by security services)

- Section 4.5 - All electric strikes (mortise and rim type) will require the installation of a diode at the end of line at the strike location. Diodes are also required when using the integration of a Camden door operating device (cx-12 plus, Cx-33, etc.)

- Section 3.4 - All ICT equipment must be installed within factory ICT enclosures.

- Section 4.1 - All AC power should be hard-wired on a dedicated 15 Amp circuit, no additional cord and plug connected device(s) should be allowed.

- Section 4.1 - Backup batteries must be installed for all ICT power supplies. Batteries must be 12v 7ah batteries and be labeled with the month and year of installation.

- Section 4.1 - All ICT equipment and security devices must be powered from the ICT power supplies in cabinets.

- Section 4.1 - When installing modules like CX-12, CX-33, wireless panic modules, wireless receiver, security voice paging system, and LED strobes. They must be powered by a ICT power supply with battery backup.
- Section 4.1 - All Locking devices must be powered from ICT power supplies.
- Section 4.1 - All Maglock must be powered from Maglock power supplies.