Electronic security installation requirements in City of Winnipeg buildings

Revision 5. July 14, 2011

Table of Contents:

Intrusion Alarm

1. System partitioning

System should be logically separated (partitioned) to effectively protect the building's perimeter and all offices and sub-divisions areas. Partition design should meet the following specifications:

a. Separate perimeter partition, which can be armed as "Stay" or "Away". If absolutely necessary the perimeter partition may have multiple designated points of entry with dedicated arming stations.
b. Separate interior partitions for all areas with different functionality. An interior partition must have a single designated point of entry with a dedicated arming station. Interior partitions should have a possibility to be armed as "Stay" or "Away"
c. Separate partitions for all points of entry inside the interior partitions, which should stay armed during the business hours and used only under special conditions (e.g. fire exit doors). This type of partitions should have separate audible notification devices (e.g. sirens, bells, horns, etc), a provision for arming and disarming, and a provision for local temporary silencing of the audible notification (if the partition is armed and disarmed remotely).
d. Each partition should have dedicated output points for Arm, Burg, System Trouble, Zone Fault, and Zone Tamper
e. Each partition should have a single or multiple audible notification devices (e.g. sirens, bells, horns, etc). The audible notification devices signal should not lose more than 40% of SPL at the most distant point due to attenuation, refraction, reverberation, etc.
f. Perimeter partition should have external weather resistant audible and visual notification devices (e.g. sirens, light strobes, etc)

2. Head end

The system's head end should meet the following requirements:

a. Hardware type used is DSC Maxsys PC4020 Series
b. The system head end should be located at a secure room accessible for authorized personnel only
c. The head end room should be located on approximately equal distance from all most outlying field devices
d. Cables from all field devices should be home-run to the head end location
e. Only ULC listed and Department of Labour approved enclosures should be used
f. All enclosures (including card access, power supply, and auxiliary interface enclosures) should have tamper switches and locks. No padlocks are accepted. Locks on all enclosures should be keyed identically.
g. All enclosures (including card access, power supply, and auxiliary interface enclosures) should be installed at serviceable heights (min 3ft – max 6ft)
h. All enclosures (including card access, power supply, and auxiliary interface enclosures) should be interconnected with electrical conduits. The size of conduits should allow for 40% future expansion
i. Only original DSC power supply transformers should be used
j. All power supplies (including card access power supplies) loads should not exceed 70% of nominal

k. All power supply transformers for any type of DSC controllers should be installed in a separate dedicated enclosures located in the same room as the controller or expander panels
l. All security equipment (including card access and auxiliary interface equipment) power supplies should be fed from a separate building power circuit connected to an emergency power source
m. No PC4020 controller should accommodate more then four logical partitions
n. PC4020 is not allowed to be a power source for anything other then the ComBus (Communication Bus) (exclusive for the primary keypad).
o. PC4204CX modules should be used to power up sirens, motion detection devices, keypads and other remote ComBus devices. PC4204CX load should not exceed 70% of nominal.
p. A dedicated PC4204CX should be used to power up all audible notification devices. PC4204CX load should not exceed 70% of nominal.
q. Each PC4020 should communicate back to the central monitoring location an AC Fail condition
r. Maximum distance from a head end controller to a ComBus communicating device (e.g. Alarm Keypad) is 750 feet.
s. A sub-panel with a ComBus repeater PC4204CX should be used on greater distances
t. All sub-panels should meet all requirements for the head end panel (except for the distancing requirement)
u. Battery backup should be installed for every controller supplied with battery backup terminals

3. Field devices and cabling
    a. General cable and field device requirements:
        - Use premium quality (e.g. Belden) stranded cables
        - All cables should be run in conduit
        - No cable splices are accepted
        - All status changing field devices should have DEOL (Double End of Line) supervision
        - All field device terminations and connections must be soldered
        - All cables should be uniquely and clearly labelled on both sides of the run. Labels should be permanent and not be susceptible to disconnection from the cable if exposed to thermal or mechanical influence.
        - All cables should be labelled in ascending order in clockwise direction relatively to the floor plan. The labelling sequence starts at the device installed by the primary entrance to the building or partition.
        - An as-built indicating all cable runs and identifying the cables should be submitted as well as the system layout diagram created with accordance to DSC design specifications.
    b. Arming Stations

- An arming station consists of a card access card reader, an LCD4501 intrusion alarm keypad enclosed inside a universal Honeywell guard TG511A1000
- Arming stations should always be installed on the secure side of partitions
- An arming station should provide for a “Stay” and “Away” indication if applicable to a partition
- A 7/8” hole must be made in the front cover of TG511A1000 aligned with a ½” hole made in the front cover of LCD4501 to allow users access to the right scroll button of LCD4501
- Arming station devices should be installed 48” from the floor level to centre to meet the accessibility requirement, and not more then 6” apart.
- 22AWG-6c cable should be used for an LCD4501 connection

c. Doors
- Normal or narrow gap GE Security 1076 series recessed type 1” door contacts should be used on all protected doors
- If two security partitions share a door, a DPDT contact should be used
- If a door monitored by both intrusion alarm and card access system door position switches, a DPDT contact should be used
- Door magnets should be installed within ¼” alignment with the door contacts
- Door magnets must always be secured by a bracket or a woodblock
- All monitored doors should comply with a “double hit” by-law. In other words, a door should always be monitored by a secondary detection device (e.g. a motion detector, a set of optical beams, etc) in addition to a door contact
- Any door contact cabling should be recessed at any transition point from the wall, ceiling, basement, etc.
- 22AWG-4c cable should be used for each door switch connection
- Overhead door position switches should be installed on the door rails 8-10’ off the ground

d. Motion detection
- All interior spaces with windows, glass walls, or other possible points of entry should be protected by motion detection devices
- Motion detection devices should be installed to have at least 20% of detection zones overlapping
- Motion detection devices should be selected to address potential issues with detection obstructions and serviceability, and provide for maximum coverage and efficiency (e.g. motion sensors designed to provide a 90 degrees coverage of a space should be installed precisely in the corner without any offsets)
- No swivel mounts are allowed for motion sensors installation
- Approved motion sensing devices are:

1. Linear and angular detection: Honeywell DT7550C model (up to 50’), Optex CX-702 (50’ and more)
2. Ceiling mount 360 degrees detection: Optex FX-360 (up to 40’), Optex SX-360Z (up to 60’)
3. Photo-electric beams: Optex AX-70/130/200TN, Optex RN4 10-25/25-75/75-150 (for higher sensitivity and security areas)

- 22AWG-6c cable should be used for each motion sensor connection

Card Access

1. System coverage
   The card access system should monitor key building perimeter access points, the points of the separation of public and staff areas, and the points of higher sensitivity and security. The system should also provide for the arming and disarming functionality of the security system.
2. Head end
   The system's head end should meet the following requirements:
   a. Johnson Controls Cardkey/Pegasys platform hardware should be used
   b. CK721 network controllers should be located in the same room as the intrusion alarm equipment if the manufacturer recommended distance requirements are met
   c. If sub-panel installation is required, it should be located at a secure room accessible for authorized personnel only
   d. Only designated JCI enclosures SEC-ENC1616/2024/2424/2430/3042WDP enclosures should be used
   e. Enclosures should be built as per JCI specifications (see Appendix 2)
   f. Tamper switches should be connected to both CK721 and intrusion alarm system tamper inputs
   g. Only Altronix power supplies in original enclosures are acceptable for energizing electrical locking devices (unless a specialized power supply must be used with a locking device). Battery backup should be installed for every power supply
   h. All power supplies should be located at the same room as controller enclosures
   i. All power supplies (including card access power supplies) loads should not exceed 70% of nominal
3. Field devices and cabling
   a. General cable and field device requirements:
      - Use premium quality (e.g. Belden) stranded cables
      - All cables should be run in conduit
      - No cable splices are accepted
      - All status changing field devices should have DEOL (Double End of Line) supervision
      - All field device terminations and connections must be soldered
      - All cables should be uniquely and clearly labelled on both sides of the run. Labels should be permanent and not be susceptible to disconnection from the cable if exposed to thermal or mechanical influence.
      - All cables should be labelled in ascending order in clockwise direction relatively to the floor plan. The labelling sequence starts at

the device installed by the primary entrance to the building or partition.

- An as-built indicating all cable runs and identifying the cables should be submitted as well as the system layout diagram created with accordance to Cardkey/Pegasys design specifications.

b. Doors

- A regular card access door must have a electric locking device, a reader, a door position switch, and a request-to-exit motion sensor
- A card-in/card-out doors installation involving usage of electromagnetic locking devices should be accompanied by a separate permit. In addition to the Building Code requirements each door should have a local vandal-proof audible notification device energized when an emergency egress protocol is used. The audible notification device signal should be only cancelled from the centralized monitoring station.
- All card readers should be installed 36” from the floor level to centre
- Approved request-to-exit device is Kantech Systems KAN-TREX XL BLK
- Approved card reader models are HID iClass R10 reader (model #6100CKN07C0) for installation on the door mullions and HID iClass R40 reader (model #6120CKN07C0) for installation on wall surfaces and single gang boxes. For applications where an extended range of RFID is required HID iClass R90 reader (model #6150AKT07C0) should be used
- MOV of appropriate nominal should be connected in parallel with the electric locking device