281316 ELECTRONIC SAFETY AND SECURITY SYSTEMS

Cornell's Design and Construction Standards provide mandatory design constraints and acceptable or required products for all construction at Cornell University. These standards are provided to aid the design professional in the development of contract documents and are not intended to be used verbatim as a contract specification nor replace the work and best judgement of the design professional. Any deviation from the Design and Construction standards shall only be permitted with approval of the University Engineer.

PART 1: GENERAL

1.01 RELATED DOCUMENTS

A. Policy 8.1 – Responsible Use of Video Surveillance Systems. Requirements for video systems, monitoring, and recording are addressed in this University policy.

B. Policy 8.4 – Management of Keys and Other Access Control Systems. Requirements of access control, by key or by card access, are addressed by this policy.

C. IT Policies 5.4.1 Security of IT Resources, 5.7 Network Registry, 5.8 Authentication to Information Technology Resources and 5.10 Information Security

D. Crime Prevention Through Environmental Design Guidelines (CPTED)

E. Lenel Onguard Hardware and Installation Manuals

F. NFPA 730: Guide for Premises Security

G. NFPA 731: Standard for the Installation of Electronic Premises Security Systems

H. Other Design and Construction Standards. The following standards are guidelines and may be of use when considering a holistic approach to security design:

1. DCS DIV 26 - Electrical (Sec Low voltage, fire alarm, etc.)
2. DCS 16530 – Site Lighting
3. DCS 02501 – Campus Landscape
4. DCS 08710 – Finish Hardware
5. DCS 16700 - Communications
6. DCS Standard Details – Communications 6.6 – Emergency Telephones

1.02 INTRODUCTION

A. This standard applies to A/E firms, design professionals, and tradespeople involved in the design, procurement, or installation of electronic security devices or systems.

B. The electronic security devices/systems encompass head-end computers, network connections (including wireless), data transmissions, communication devices, multiple points of monitoring, interfacing controls, sensors, and actuators. Some functions may be supported locally as well as University-supported.

C. This standard applies to all new construction and renovations projects, as well as single device installations on the Ithaca campus and any other location or campus subject to University Policies 8.1 and 8.4.

D. For the purposes of this standard, electronic security systems or devices include:

1. Access control (wired and wireless).

2. Networked video surveillance.

3. Intrusion detection.

4. Blue lights phones & Emergency phones (*refer to DCS Standard Details – Communications 6.6 – Emergency Telephones*).

E. Per University Policies 8.1 and 8.4, security and access control systems must be integrated with the University central systems unless an exemption has been granted.

1. For ***Access Control and Video Surveillance systems***: CUPD Access Control shall be consulted during initial design or planning, during schematic and construction design reviews, during construction if a scope change occurs or clarification is needed, and prior to building occupation/building signoff for an Access Control commissioning and for video transmission testing.

2. For ***Intrusion Detection system, Blue Light and Emergency phones***, CUPD Crime Prevention shall be consulted during initial design or planning, during schematic and construction design reviews, during construction if a scope change occurs or clarification is needed, and prior to building occupation for testing of alarms into the CUPD Telecommunications Center.

   a. Any device that generates an alarm to the Cornell Police must be pre-approved by the Chief of Police before any estimate or work is done.

F. Electronic security systems/devices are not to be connected by hardware, integrated by software, or otherwise interfaced with any other control systems (ex. Building Automation Control System) or life safety systems except where specifically required by code or approved by appropriate system owner and CUPD Access Control Program.

G. Electronic security systems/devices planning should be incorporated into the overall building design. Physical security devices and measures, as well as electronic devices and connections, are to be considered at the same time as comfort, function, energy efficiency, maintainability, life safety, accessibility, environment, inspiration and any other primary feature attributed to a facility.

1.03 QUALITY ASSURANCE

A. The design of all security and/or access system installations shall be performed by a qualified individual, either licensed as a Professional Engineer or certified as a security professional. Consultant shall provide credentials to the Cornell project manager upon request.

B. The integrated security and/or access system including all equipment, components, and accessories shall be UL listed for this purpose.

C. The Contractor providing the security and/or access system must be certified Lenel Level II (Lenel Silver Certification) or greater and licensed by New York State to install security and access control systems.

D. The Contractor installing the electronic security hardware must be certified in the installation of the appropriate devices.

1.04SYSTEM DESIGN

A. CUPD Access Control Program must assess all video installations and re-positioning of cameras *prior* to the start of any project to determine the appropriate model and specifications.

B. Coordinate the following elements into Basis of Design:

1. List applicable Codes and Standards. Identify Building Occupancy Type

2. Type of security or access system.

3. Sequence of operation on all electrified devices (especially when fire alarm and access control systems are interconnected)

4. Wiring type shall be per manufacturer's specification.

5. Main equipment shall be located in a secured area and in a locked enclosure.

6. Special considerations. For example, when a facility houses animals, a Cornell Center for Animal Resources and Education representative, must also be consulted.

C. Drawings and Specifications shall include all requirements for Submittals and for As-Built information. Submittals shall contain the following information:

1. Product information for all installed components

2. Door riser diagram with typical equipment and device connection and labeling. (A detailed connection diagram is *not* required until project completion)

3. System/Building riser diagram with reader module and intelligent system controller connections detailed and labeled

4. Wire schedule

5. Battery stand-by and system load calculations

6. Special system requirements (interlocks with other systems, for example)

7. System labeling materials and methods

1.05 SUBMITTALS

A. To ensure compliance with the intent of this standard, all system final designs and associated contract submittals shall be reviewed by Facilities Engineering and CUPD.

B. One (1) copy of each new project submittal shall be sent to both FE and CUPD for review and comment prior to releasing final approved submittals to the contractor.

PART 2: MATERIALS AND EQUIPMENT

2.01 SYSTEM DESCRIPTIONS

A. Card Access Systems

1. Wired

a. Card Access Systems (CAS), at the User End, are comprised of card reader, door contacts, electric hinge or power transfer (wired systems), door strike, latch, reader interface module, interconnecting power and communication wiring, head-end intelligent system controller. All systems, unless exempted from University policy, are centrally monitored transmitting data to and received by CUPD Access Control Services.

2. Wireless

a. Schlage AD400 – is comprised of an AD400 lockset, PIM400-1501 RSI wireless access point, communication wiring with power over Ethernet, and must be installed with an eight-cell battery pack. Every PIM must be installed with an external antenna. The series of AD400 installed must support a secure credential. Cornell IT policies must be adhered to when attaching devices to the University network.

B. Video Surveillance Systems (NVSS)

1. At the User End, are comprised of IP-enabled cameras, interconnecting power and communication wiring via POE (power over Ethernet). Cameras must be connected to a POE-enabled switch with ports enabled on the appropriate security VLAN except where approved by CUPD Access Control. All systems, unless exempted from University policy, are capable of being centrally monitored transmitting data to the central VMS. Some systems are also locally monitored within a specific unit.

2. Minimum Camera Requirements:

a. Every Camera installation must first have an assessment completed by CUPD Access Control Program to determine a device suitable for the requirements.

b. 8 frames per second.

c. Support for 32GB SD card.

C. Intrusion Detection Systems (IDS)

1. At the User End, are comprised of panic push button, motion detectors, door contacts, interconnecting communication wiring and head end intrusion dialer panel. Installation of panic push button systems require prior consent and approval from the Chief of Police.

2. A phone circuit must be available/provided for communication to the University receiver. All systems transmit data to and are received by CUPD Telecommunications Center. Reporting format, unless otherwise approved by CUPD Telecommunications Center, will be contact ID.

D. Blue Light Phones

1. Blue light phones are ring down phones that are located throughout campus for use in case of emergencies. Blue light phones are located outside of campus buildings and attach to a metal pole with a blue light mounted above. Some blue light phones are positioned on the exterior side of a building with a corresponding blue light above.

2. Each blue light has a conduit for a dedicated power circuit and a separate conduit for the voice and data. Conduit for the voice cabling shall terminate in the nearest building. A 12 AWG (min) ground wire shall be available for primary protection bonding.

3. Blue light emergency telephone detail – (*refer to DCS Standard Details – Communications 6.6 – Emergency Telephones*)

4. The blue light phone enclosure is a yellow metal box type enclosure and shall be installed to meet ADA specifications. Each blue light phone is assigned a PX number for location referencing.

    a. Blue Light phone enclosure is a Ramtech 926D part# 912OSHA Yellow.

    b. Blue light phone is Ramtech R733 telephone part # R733.

    c. All blue light phone installations must adhere to ADA specifications.

E. Emergency Phones

1. Emergency phones are designed to perform the same function as a blue light phones, but are located inside buildings.

2. Emergency phones shall be yellow in color for higher visibility and do not have a keypad for dialing purposes. Emergency phones shall ring directly to the Cornell University Police Department.

3. Emergency phones shall be provided on all levels of the facility and located not more than 20 ft. from each exit. Additional emergency ring-down phones shall be placed so that travel distance does not exceed 200 ft.

4. Each emergency phone must have its own dedicated voice circuit.

5. Emergency phones used shall be the Viking 1600A.

6. These instruments will be located to meet ADA requirements for height and clearance and have required signage.

7. Deviations shall be at the direction of Risk Management, Environmental Health & Safety, Cornell Police and/or Network & Communications Service engineering.

F. Card Access, Video and Intrusion Head-End Servers (HDS)

1. The Head-End Database Server (HDS) warehouses the total University client information. This server supports Lenel OnGuard Software System.

2. The Head-End Database Server (HDS) stores all alarms, trouble conditions, asset management information, administrative information, video management information, etc. delivered from the intelligent system controllers (ISCs) on campus across the TCP/IP connections. The historic alarms are kept for a minimum period of three months and then they are archived.

G. Existing non-OnGuard Supporting Security

1. Ties into the CUPD central station manufactured by Bosch. These existing non-OnGuard supporting systems report to the CUPD Central Station over dedicated copper communication pairs in the respective building. A digital dialer located in or at the building's security, access system transmits the information.

2. The CUPD Central Station security output is gathered and transmitted over a TCP/IP connection to the HDS to ensure integrity of alarms and trouble conditions. Digital dialers must be Honeywell unless approved by FM Operations Fire/Alarms & Security Technician.

H. Card Access, Video and Intrusion Campus Police Workstation (CPW)

1. A Campus Police Workstation (CPW) supporting the campus security systems resides at Barton Hall. This terminal supports Lenel OnGuard Software System. Cornell IT policies must be adhered to when attaching devices to the University network. See Part 1.01 Related Documents

2. The CPW monitors only certain critical alarms and trouble conditions from intelligent system controllers (ISCs) located in Cornell University's buildings. This system does not monitor routine transactions.

3. Arrangements should be made with the Cornell Police to enable monitoring of the critical alarms. Alarms will only be responded to after CUPD has been satisfied that the location(s) in question have passed their certification process. This process should occur during the commissioning phase of the project.

4. CUPD Telecommunications and Crime Prevention should be engaged throughout the process of design to provide feedback.

5. New installations of OnGuard supportive ISCs shall be tied into the Head-End Database Server (HDS) through a secure TCP/IP network connection. Only designated IP addresses will be allowed to access the HDS.

6. Existing non-OnGuard supported security and access systems tie into the Head-End Database Server (HDS) through a dedicated TCP/IP network connection from Cornell's Central Station manufactured by Bosch.

I. Campus User Workstations

1. Client Workstations (CWs) can be located in the building or remotely. These terminals support the RemoteApp application delivery method. Through RemoteApp, they are able to access the Lenel OnGuard Software System. The CWs selectively monitor alarms, trouble conditions, asset management information, administrative information, video management information, etc. delivered from the HDS. They can also be used to modify administrative information such as grant access levels to cardholders, define time zones, and generate reports.

2. Client Workstations can access the VMS through a web browser.

2.02 SYSTEM OPERATION AND PERFORMANCE

A. System operation and performance shall include, but not be limited to, the following features:

1. Proper activation of door hardware when a valid credential is presented.

2. Appropriate shunting of the alarm upon exit from secured space.

3. Video signal being transmitted over IP.

4. Alarm initiation.

5. Trouble initiation.

6. Activation of alarm notification.

7. Activation of trouble notification.

8. Activation of fire safety functions.

9. Total supervision, monitoring of abnormal conditions in the system.

10. Activation of off-premise signals that are sent to the HDS via the Bosch Central Station (existing non-OnGuard supported systems) or Ethernet (OnGuard supported systems).

B. Activation of the fire alarm system shall cause the following:

1. Electric door hardware located on egress doors to lose power and allow egress/ingress where required by fire code.

2. Electrical door hardware mounted to a fire door must close and latch upon activation of the fire alarm system.

3. Delayed egress device must deactivate.

C. Activation of any security device producing an alarm or trouble shall cause, but not be limited to:

1. Transmission of the alarm or trouble signal to the Building ISC(s).

2. Transmission of the selected alarm or trouble signal to the Head-End Database Server (HDS).

3. Indication of the alarm or trouble condition at the computer monitor display at the CW, CPW, and HDS shall include the alarm or trouble description, time/date, building controller, device, input/output, priority code.

D. Activation of any card access device shall cause, but not be limited to:

1. Transmission of the data signal to the Building ISC(s) and HDS.

2. Indication of the data signal including the alarm or trouble description, time/date, building controller, device, input/output, card, and priority code by the computer monitor display at the CW and HDS.

E. Items C and D above define normal operations. In the event of a communication failure between an ISC and the HDS, these signals will be stored and forwarded to the HDS when the communication is restored.

2.03 POWER REQUIREMENTS

A. Provide 120VAC power to the system power supply locations. Where available, provide a dedicated emergency power circuit.

B. Provide 12VDC power supply for card access boards, and 24VDC power for other devices (crash bar, door hardware).

C. Power supply must be per hardware manufacturer's specification.

D. Varying voltage supplies should be kept separate from each other.

E. Panel power supplies must be kept independent of all other components and should be connected to the power supply monitor on the panel where available.

F. Locking hardware should be directly wired to a distribution board; never a series.

G. Battery backup is required for all intrusion, video surveillance and card access systems must be replaced a minimum of every 3 years.

H. The Engineer of Record shall provide power calculations, including load capability and maximum load per power supply, to Cornell Facilities Engineering during the submittal process and at the completion of the project.

2.04 BATTERY BACK-UP POWER SUPPLY

A. Battery Back-Up Power Supply – Access Control Systems

1. Batteries shall be of the sealed, lead-acid type.

2. Batteries shall be capable of providing operating and supervisory power to meet the requirements of NFPA 731 latest adopted version.

3. Batteries shall be capable of providing operating power to operate the system for a minimum of 24 hours, and at the end of that period, shall be capable of operating all alarm sounding devices for 15 minutes, where required.

4. Batteries shall be mounted in the control panel or a separate enclosure of similar type to the main control panel.

5. The Engineer of Record shall provide battery calculations to Cornell Facilities Engineering during the submittal process and at the completion of the project.

6. Batteries should be set up on a preventive maintenance cycle and should be tested/replaced every 2-3 years depending on use.

7. ISC Coin cell battery must be replaced at a minimum of every three years or whenever maintenance is completed on the controller.

B. Uninterrupted Power Supply – Video Surveillance Systems

1. Capable of providing 60 minutes for all connected devices.

2. The Engineer of Record shall provide battery calculation to Cornell Facilities Engineering during the submittal process and at the completion of the project.

3. Batteries should be set up on a preventative maintenance cycle and should be tested/replaced every 2-3 years depending on use.

2.05 CABLE AND RACEWAY SYSTEMS

A. Installations shall be performed to the current code requirements.

B. Cables shall be routed in raceway systems. Plenum cable is not acceptable.

C. Raceway systems shall be installed in a concealed manner; they shall be brought in above an accessible ceiling and fished inside the walls. Surface raceway systems are permitted where ceilings are inaccessible and walls cannot be fished.

D. Cabling shall be run in such a fashion to be kept at least 18" away from electric or data lines. In the event that a cable must cross over the path of an AC line, the cable must cross the path at a 90-degree angle to the AC line, thus keeping EMF interference to a minimum. Cabling must be kept at least 18" away from fluorescent lighting ballasts.

E. Cornell University Facilities Engineering (FE) must approve any deviations in wire, raceway systems, or raceway hardware.

F. Raceways shall be run from the field device to the head-end termination point in a professional manner, utilizing conduit, beam clamps, or other devices where necessary. In areas where the raceways are to be run above the drop ceiling, conduits shall be routed together where possible. Routing shall be in a competent manner, with raceways mounted so as not to interfere with the servicing of other building infrastructure systems in the future. Electrical work shall conform to the latest local codes and the National Electric Code (NEC).

G. Specifications for Ethernet cabling:

1. All cable should comply with CIT cabling standards, be full copper and a minimum rating of CAT6 CCA (Copper Clad Aluminum) cabling shall not be used.

2. All cabling should adhere to current NFPA and NEC requirements for power over Ethernet.

H. Communication conductors shall be shielded twisted pairs; a minimum 24 AWG./2-pair stranded copper between the ISC and each downstream device. Manufactured by Belden, model #9842 or equivalent.

I. Low-voltage power conductors shall be unshielded twisted pairs; a minimum 18 AWG./4-conductor stranded copper between the power supplies and each downstream device. Manufactured by Belden, model #9157, or equivalent.

J. Card reader conductors shall be a minimum of 22 AWG./6-conductor, shielded, between card reader and reader interface. Belden model #9942 or equivalent.

K. Egress device conductors shall be a minimum of 22 AWG./2-conductor between egress device and reader interface module. Belden model #8442 or equivalent.

L. Door position switch conductors shall be a minimum of 22 AWG./2-conductor between egress device and reader interface module. Belden model #8442 or equivalent.

M. Electric locking hardware conductors shall be a minimum of 18 AWG./2-conductor, between head-end power supplies and each downstream device. Belden model #8461 or equivalent.

N. Security and Card Access wiring shall be installed in a separate conduit system independent of other system circuits. This excludes Ethernet cable that can be run in existing data conduit.

O. System wiring, circuits, and conductors shall be identified by number at termination points (i.e., control panels, remote annunciators, etc.) and splice points (i.e., junction boxes, splice boxes, etc.).

P. Junction and splice boxes containing card access system wiring, circuits, and conductors shall have blue covers.

Q. End-of-line resistors shall be installed at the location of the door contact or other sensor, not at the ISC.

2.07 DOOR HARDWARE

A. New door installations, opening hardware must conform to the current Americans with Disabilities Act guidelines; either lever set, flip paddle, panic paddle or crash bar hardware is acceptable.

B. Hinges on reverse beveled doors shall be non-removable pins (NRP).

2.08 ELECTRONIC LOCKING HARDWARE

A. Use of magnetic locking hardware, electric strikes and standalone keypad locks is not permitted without obtaining an exemption from FM Operations Lock Shop Technician, CUPD Access Control and the Director of Risk Management.

B. Electronic hardware in the building shall use one standard voltage. Applications shall operate on 24VDC voltage. Deviations from this voltage are unacceptable without prior written consent by the University's FM Operations Fire/Alarms & Security Technician and FM Operations Lock Shop Technician. Existing electronic hardware that is not feasible to replace is an acceptable reason to deviate from this voltage. In applications where the latch bolt of the locking mechanism can be accessed from the outside of the door, a latch guard, or astragal, must be installed over the locking mechanism to prevent retraction of the latch bolt, allowing release of the door to an open condition.

C. Electronic locking hardware must be installed in a fail-secure configuration.

D. Delayed egress devices must release to an unlocked position on any fire alarm activation where required by local fire or building codes.

E. Fail-Safe operation will be permitted only in instances where dictated by local fire or building codes.

F. On fire rated doors, latch retraction mechanisms must release to latched position and magnetic door hold open devices must release upon receipt of a signal from the building fire alarm system.

2.09 INTELLIGENT SYSTEM CONTROLLERS (ISCs)

A. General

1. The project is responsible to pay the costs associated with providing the dedicated TCP/IP network connection to each ISC location. Request for data must be submitted by the end user or Project Manager at a minimum of two weeks prior to installation. Request should include project account number and monthly billing number. Access Control Program to provide VLAN information.

2. Use of existing or single Intelligent System Controller (ISC) is preferred. Multiple ISCs are acceptable when specifically requested by the customer or approved in design by the CUPD Access Control Project Manager.

3. The integrated system including equipment, components, and accessories shall be UL listed for the purpose for which the equipment, components, and accessories are used.

B. Enclosures

1. Enclosures shall be of the 22 ga. heavy-gauge, galvanized steel, dead-front construction with keyed, lockable panel cover type.

2. FM Operations Fire/Alarms & Security Group must approve panel locations.

3. All panels must have tamper switches on the enclosure wired to the cabinet tamper inputs on the controller board.

C. Intelligent System Controller Modules:

1. Host communications shall be direct wire TCP/IP, flash memory for real-time updates, with a minimum of 16MB onboard memory expandable to 64MB. The TCP/IP is over Ethernet at a minimum of 100mbps.

2. Supports up to eight different card formats, with issue code support for both Wiegand and magnetic formats.

3. Will support at least 64 readers or 32 downstream devices, and minimum 50000 cardholders, 255 access levels, 255 Holidays with grouping, 255 time zones, each with 6 time intervals.

4. Alarm Masking, Individual shunt times, available 6-digit pin code.

5. Two dedicated inputs for tamper and power failure status.

6. Manufacturer: Lenel LNL-X3300, Lenel LNL-X2220 or Lenel LNL-X2210. (Use the Lenel LNL-X2210 only for Schlage AD400).

2.10 INPUT CONTROL MODULES

A. General

1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.

2. Two inputs are available for cabinet tamper and power fault monitoring. Normally, the contacts are closed. Power fault monitoring should always be in place. The cabinet tamper may be shorted if not necessary.

3. Alarm inputs shall be supervised with end-of-line resistors that are 1000 ohm, 1% tolerance.

4. The Input Control Modules are intended for low voltage, class 2 circuits only.

B. Cabinet

1. Refer to ISC requirements for Input Control Module cabinet requirements.

C. Input Control Module:

1. Line supervision, with 12VDC power supply.

2. RS-485, 4-wire communications.

3. Sixteen programmable supervised input contacts (use end-of-line resistors).

4. Two form-C 5A, 30VDC contacts for load switching with contact protection.

5. Two dedicated inputs for tamper and power failure status.

6. Manufacturer: Lenel LNL-1100 or Lenel LNL-1200.

2.11 OUTPUT CONTROL MODULES

A. General

1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.

2. Two inputs are for cabinet tamper and power fault monitoring.

3. Contact protection shall be used to minimize premature failure of the contacts and to increase system reliability.

4. The Output Control Modules are intended for low voltage, class two circuits only.

B. Cabinet

1. Refer to ISC requirements for Input Control Module cabinet requirements.

C. Output Control Module

1. Line supervision with 12VDC power supply.

2. RS-485, 4-wire communications.

3. Sixteen form-C 5A, 30VDC contacts for load switching that support “on”, “off”, and “pulse” control.

4. Two dedicated inputs for tamper and power failure status.

5. Manufacturer: Lenel LNL-1200.

2.12 SINGLE READER INTERFACES (SRIs)

A. General

1. Dual Reader Interfaces (DRI) are preferred whenever possible due to greater functionality and expansion potential. See section 2.13 below.

2. Locate its respective power source as close as physically possible, while maintaining proper service clearances.

3. Two supervised inputs are for exit request (normally open) and door contact (normally closed) monitoring.

4. Alarm inputs shall be supervised with end-of-line resistors that are 1000 ohm, 1% tolerance.

5. Two output relays support fail-safe and fail-secure operation. One relay shall be used for the strike (locking device) and is capable of 5A; the other relay may be used for auxiliary functions and is capable of 1A.

6. Provide end-of-line termination at the end of the communications line. If the Single Reader Interface is at the end of the RS-485 line, the J4 termination jumper must be set.

B. Power

1. Provide a 12VDC, 125mA power input.

2. 80mA is available from Single Interface Reader for reader TTL power.

3. Circuit with 18AWG (minimum) twisted pair cable.

C. Upstream Communication

1. Port 1, using 2-wire RS-485 interface, is used to communicate with the Intelligent System Controller.

2. RS-485 interface cable shall be a minimum 24 AWG twisted shielded pair.

3. Cable drops to devices from the Single Interface Reader should be kept to a minimum.

D. Manufacturer: Lenel LNL-1300.

2.13 DUAL READER INTERFACE MODULES (DRIs)

A. General

1. Locate its respective power source as close as physically possible, while maintaining proper service clearances.

2. Eight supervised inputs, four per door. Inputs per door are for exit request (normally open), door contact (normally closed), and two auxiliary monitoring points (selectable through the software).

3. Alarm inputs shall be each supervised with two end-of-line resistors that are 1000 ohm, 1% tolerance for a total of 2000 ohms.

4. Six output relays support fail-safe and fail-secure operation. All six relays are capable of 5A apiece. Relays per door are for the strike and two auxiliary relays.

5. Provide end-of-line termination at the end of the communications line. If the Dual Reader Interface is at the end of the RS-485 line, the J5 and J6 termination jumpers must be set.

B. Power

1. Provide a 12VDC, 450mA power input.

2. 80mA is available from Dual Interface Reader for reader TTL power.

3. Circuit with 18AWG (minimum) twisted pair cable.

C. Upstream Communication

1. Port 1, use 2-wire RS-485 interface, used to communicate with the Intelligent System Controller.

2. RS-485 interface cable shall be a minimum 24 AWG (minimum) twisted shielded pair.

3. Cable drops to devices from the Dual-Interface Reader should be kept to a minimum.

D. Manufacturer: Lenel LNL-1320.

2.14 CARD READERS

A. The card readers shall be installed on the unsecured side of the door. It can be mounted adjacent to the door, on the door, or pedestal mounted. The reader shall be mounted in accordance with current ADA Compliance guidelines.

B. For double door installations, the inactive door must be monitored with door position switches.

C. All doors with electrified locking hardware must have the request to exit (REX) built into the hardware and a door position switch.

D. If a door operator is in use, the reader must be mounted adjacent to operator paddle.

E. All doors must have key override.

F. All-in-one door mounted units are approved for both interior and exterior doors not requiring door operators.

G. Multi-technology readers must be used and at a minimum must support 125KHz proximity and 13.56 MHz (iClass, MIFARE, DESFire). Additionally, where available, low power Bluetooth support should also be specified.

H. In the case of Assa Abloy products, this is typically specified by calling out the BIPS credential.

2.15 INTRUSION DETECTION CONTACTS

A. On standard person doors, the contact shall be mounted in the top of the doorframe, 4-6" from the lock edge of the door.

B. The electronic configuration for IDS contacts is normally closed and supervised.

2.16 EGRESS MOTION DETECTORS

A. Use of motion detection for egress is unacceptable without obtaining an exemption from CUPD Access Control, FM Operations Lock Shop and the Director of Risk Management.

B. If approval is given:

1. Egress motion detectors shall be ceiling mounted whenever possible. When the detector must be wall or frame mounted above the door, it will be angled down as far as possible, to provide the proper coverage.

2. The coverage pattern shall reach from the detector to the level of the floor, and shall not protrude more than 12" out from the surface of the door, nor more than 6" past the doorframe on either side. Masking of the detector is acceptable to meet the coverage pattern.

2.17 ACCEPTABLE MANUFACTURERS

A. The equipment, components, and accessories shall be as specified in the contract documents. Requests for authorization to substitute, vary or change the specified equipment, components or accessories of the approved manufacturer must be submitted, in accordance with Cornell University's General Requirements.

2.18 IDENTIFICATION

A. Provide lettered phenolic identification plates on the following equipment, components, and accessories as noted below:

1. Building Intelligent System Controllers (ISCs)

2. Control Modules

3. Interface Modules

4. Remote Power Supplies

5. Provide computer-generated adhesive labels on system devices (Brady, Dymo, P-Touch).

    a. The label shall indicate the address and must be located on the device or adjacent to the device if this is not practical.

B. Cabling and devices terminating at the control equipment shall be appropriately labeled with the proper device number or device description. Terminal blocks that are active shall be labeled with their appropriate landing site on the terminal board.

C. System Labeling and Identification

1. The description in the notes field of the OnGuard access control system shall indicate the location of the ISC's, DRI's, power supplies, PIM's, SRI's, and Video devices and include the date of installation.

2. The location shall include the room number and geographic location in the room itself.

D. Identification Plates and Labels shall be as follows:

1. ISCs shall be labeled ISC–U, where U is a value from 1-9.

2. DRIs shall be labeled DRI–UVWX, where U indicates its respective ISC numeral; and V is the ISC's respective buss, a value from 1 to 4; where WX are values from 01 to 32.

3. Devices shall be labeled UVWXYZ, where U indicates its respective ISC numeral; and V is the ISC's respective buss, a value from 1 to 4; WX indicates its respective panel, values from 01 to 32; Y indicates the input or output terminals, a value of 1 for input and 0 for output; and Z indicates its respective input or output terminal, a value from 1 to 4.

4. Examples

    a. ISC-2 is the second Intelligent System Controller in the building.

b. RIM-2305 is the fifth Dual Reader Interface served from the third buss of the second Intelligent System Controller in the building.

c. Device #230503 is the device on the third output of the fifth panel served from the third buss of the second Intelligent System Controller in the building.

PART 3: EXECUTION

3.01 MOUNTING REQUIREMENTS

A. Equipment shall be mounted in a manner consistent with the ability to work around such equipment, and to perform the normal duties required in that area without coming into contact with the control equipment.

B. Control equipment shall be mounted at a convenient height for future servicing. Control equipment shall be mounted in such a way that shall prevent their disengaging, by either vibration, gravity, or an individual unplugging them.

C. Control equipment shall have at least 4 inches of clearance from any non-system component or structure, unless mounted adjacent to another access control panel.

D. Power transformers shall be mounted in such a way that shall prevent their disengaging, by either vibration, gravity, or an individual unplugging them.

3.02 SYSTEM PROGRAMMING – CARD ACCESS

A. Cornell's Access Control Program (ACP) will perform the initial setup programming prior to the installation.

1. Facilities Fire Alarms & Security Technician or a Lenel-certified installer will perform all required wiring and terminations on the board prior to ACP configuration.

2. ACP will perform initial setup programming to include:

a. ISC configuration and labeling.

b. Device hardening.

c. User/Password configuration

d. Creation of the device instance in the access control software.

3. Facilities Fire Alarms & Security Technician or a Lenel-certified installer will:

    a. RIM (reader interface module) configuration and labeling.

    b. Initial test Time Zones and Access Levels.

    c. Creation or modification of the Emergency Response access level using the following naming convention (EMERGENCY RESPONSE – Segment Name).

B. The building/unit access control coordinator (ACC), for the building implementing the security and access measures, shall supply CUPD Access Control Project manager with the information pertaining to the desired theory of operations for the space including population residing within, and the traffic patterns and times of operation therein. If it is determined that the authorized ACC's are failing to comply with policies or misusing the system, their privileges may be revoked.

C. The security system installer is responsible for initial alarm programming and commissioning for intrusion devices with approval and collaboration of Cornell Police Telecommunications and CUPD Crime Prevention.

3.03 SYSTEM PROGRAMMING – VIDEO SURVEILLANCE

A. Cornell's Access Control Program (ACP) will perform the initial setup programming prior to the installation.

1. The project will provide ACP with the devices prior to installation.

2. ACP will perform initial setup programming to include:

    a. Camera configuration and labeling.

    b. Device hardening.

    c. User/Password configuration.

    d. Creation of the device instance in the video management software.

3. Facilities Fire Alarms & Security Technician or a certified installer will:

    a. Mount the device.

    b. Assist ACP with camera positioning during commissioning.

B. The building/unit Network video surveillance system operator (NVSSO), for the building implementing the security measures, shall approve camera views during commissioning.

1. NVSSO and their designees will be trained for local management by CUPD Access Control manager. Access to the system will not be granted until training and completion of the authorization and activation forms has occurred.

2. Authorization forms must be in place prior to this training.

3.04 TESTING, COMMISSIONING AND ACCEPTANCE

1. A final test of the respective security and card access equipment and hardware shall be performed prior to considering the installation "complete". In the case of a new building or renovation, this shall be done prior to building occupation.

2. Installation's project and/or construction manager shall schedule a systems commissioning with the Access Control Project Manager, Security Contractor/Installer, and Electrical contractor when applicable, two weeks prior to the completion of the installation of a tentative testing date. On that date, a full system test will be performed according to these guidelines.

3. The CUPD Access Control Project Manager will give a commissioning report to the project manager after the test has been completed. When a portion of the system fails during the test, that portion, or the entire system will be tested again. The extent of the retest shall be up to the discretion of Access Control Project Manager.

4. If occupation occurs prior to Access Control commissioning, the Cornell Project Manager is responsible for obtaining CUPD approval and building occupants must be notified of potential security risks (by flier, email via the Unit/College department).

3.05 WARRANTY

A. A warranty shall be provided for labor/workmanship and on hardware included in the installation, for a period of one (1) full year from the date of completion.

3.06PROJECT CLOSE OUT

A. At completion of the project, the Contractor shall provide the Cornell Project Manager with a complete set of security system "As-Built" drawings that includes, but is not limited to, the following information prior to the closeout of the project. The project manager will ensure these documents are delivered to Facilities Inventory Group for archiving.

1. Head end equipment location and interface panel locations.

2. Power supply locations.

3. Battery calculations.

4. Device locations.

5. Circuit breaker locations: Include power panel and circuit numbers.

6. Complete system riser diagram that depicts all wiring, components, and interconnections. Include locations and labeling.