1.01 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, and

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**: Cornell University Police Department (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. (See **Cornell CUPD Access Control Consultation/Installation Procedure**.)

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. (See **Cornell Police Alarm Monitoring Procedure Form**.)

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 unless 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.

1.02 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. Crime Prevention Through Environmental Design Standards (CPTED)

D. Lenel Onguard Hardware and Installation Manuals

E. CUPD Access Control Consultation/Installation Procedure

F. CUPD Alarm Monitoring Procedure

G. NFPA 730: Guide for Premises Security

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

I. Other Design and Construction Standards. The following standards are guidelines and may be of use when considering a holistic approach to security design:
   2. Design & Construction Standard 087100 – Finish Hardware
   3. Design & Construction Standard 270000 – Communications
   4. Cornell Standard Detail 6.6 – Emergency Telephones

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.
1.04 SYSTEM DESIGN

A. For all renovations and new-construction projects, consultant shall engage CUPD, Facilities Engineering, and CIT stewards.

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 (especially when fire alarm and access control systems are interconnected).
4. Wiring type.
5. Main equipment locations.
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. System riser diagram with typical equipment and device connection and labeling. A detailed connection diagram is not required until project completion.
3. Wire schedule.
4. Battery stand-by calculations.
5. Special system requirements (interlocks with other systems, for example).

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 (FE) 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 (CAS)
1. Wired: (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, PIM400-485 RSI wireless access point, interconnecting power and communication wiring, and a head-end intelligent system controller.
   b. Sargent V.S2 – is comprised of a V.S2 lockset. Special consideration must be taken to verify the presence of adequate 802.11 networking.

B. Networked 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 unless approved by CUPD Access Control. All systems, unless exempted from University policy, are capable of being centrally monitored transmitting data to and received by CUPD Telecommunications Center. Some systems are also locally monitored within a specific unit.

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. 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 circuit. If designated, additional conduit may be required for data transmission. Conduit for the voice cabling shall terminate in the nearest building. A 12 AWG (min) ground wire shall be available for primary protection bonding.

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 phone, but are located inside buildings.
2. Emergency phones should be yellow in color for higher visibility and do not have a keypad for dialing purposes. These phones ring directly to the University Police Department.
3. These 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. Emergency phones used will be the Viking 1600A.
5. These instruments will be located to meet ADA requirements for height and clearance and have required signage.
6. 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 Database Servers (HDS)

1. The HDS warehouses the total University client information. This server supports Stanley Security Solutions’ BASIS Software System and uses an Oracle database platform.
2. The 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 period of three months and then they are archived.
G. Existing non-BASIS supporting security

1. Tie into the Campus Police Workstation via Cornell’s Central Station manufactured by Bosch. These existing non-BASIS 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 or access control system transmits the information. 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 Central Shops 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 Stanley Security Solutions’ BASIS Software System. 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. 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. CUPD Telecommunications and Crime Prevention should be engaged throughout the process of design to provide feedback.

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

   b. Existing non-BASIS supported security and access systems tie into the CPW via 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 Citrix Receiver application delivery method. Through Citrix, they are able to access Stanley Security Solutions’ BASIS 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.
2.02 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.
   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-BASIS supported systems) or Ethernet (BASIS supported systems).

B. Activation of the fire alarm system shall cause, but not be limited to, electric door hardware located on egress doors to lose power and allow egress where required by fire code.

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) and the Client Workstation(s) (CW).
   2. Transmission of the selected alarm or trouble signal to the Cornell Police Workstation (CPW), and 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), the CW 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, readers, door hardware).

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

D. Panel power supplies must be kept independent of all other components.

E. Locking hardware should be directly wired to a distribution board.

F. Battery backup is required for all intrusion and card access systems.

G. 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.

H. Battery Back-Up Power Supply
   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, & 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.

2.04 CONDUIT, WIRE AND BOXES

A. Security and Card Access wiring shall be installed in a separate conduit system independent of other system circuits. Plenum-rated cable is not acceptable.

B. Communication conductors shall be shielded twisted pairs; 24 AWG/2-pair stranded copper between the ISC and each downstream device. Manufactured by Belden, model #YR48837 or equivalent.

C. Low-voltage power conductors shall be unshielded twisted pairs; 18 AWG/4-conductor stranded copper between the power supplies and each downstream device. Manufactured by Belden, model #6302UE, or equivalent.
D. Card reader conductors shall be a minimum of 22 AWG/6-conductor, shielded, between card reader and reader interface. Belden model #6504FE or equivalent.

E. Egress device conductors shall be a minimum of 22 AWG/4-conductor between egress device and reader interface module. Belden model #6541FE or equivalent.

F. Door position switch conductors shall be a minimum of 22 AWG/4-conductor between egress device and reader interface module. Belden model #6541FE or equivalent.

G. Electric locking hardware conductors shall be a minimum of 18 AWG/2-pair, between head-end power supplies and each downstream device. Belden model #6300FE or equivalent.

H. 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.).

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

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

K. 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.

L. 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.

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

2.05 CARD ACCESS SYSTEM (CAS) 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

B. Provide computer-generated adhesive labels on system devices (Brady, Dymo, P-Touch).
   1. The label shall indicate the address and must be located on the device or adjacent to the device if this is not practical.
   2. 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. 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.

2.06 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. Existing hinges located on the unsecured side of a door must be pinned with tamperproof screws or roll pins.

2.07 ELECTRONIC LOCKING HARDWARE

A. Use of magnetic locking hardware or electric strikes is not permitted without prior approval of Central Shops Lock Shop Technician and CUPD Access Control.
B. Electronic hardware in the building shall use one standard voltage. Applications should operate on 24VDC voltage. Deviations from this voltage are unacceptable without prior written consent by the University’s Central Shops Fire/Alarms & Security Technician and Central Shops 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 latchbolt 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. Hardware 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.

2.08 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.
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. Central Shops 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 wired TCP/IP, flash memory for real-time updates, with 16MB onboard memory expandable to 64MB. The TCP/IP is over Ethernet at a minimum of 10 mbps.
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.
5. Two dedicated inputs for tamper and power failure status.
6. Manufacturer: Lenel LNL-3300, or Lenel LNL-2220.

2.09 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-CS 5A, 30VDC contacts for load switching with contact protection.
5. Two dedicated inputs for tamper and power failure status.

2.10 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. Normally, the contacts are closed. Short the inputs if not used.
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.

2.11 SINGLE READER INTERFACES (SRIs)

A. General:

1. Dual Reader Interfaces (DRI) are preferred whenever possible due to greater functionality and expansion potential. (See also 2.12.) Locate its respective power source as close as physically possible, while maintaining proper service clearances.
2. Two supervised inputs are for exit request (normally open) and door contact (normally closed) monitoring.
3. Alarm inputs shall be supervised with end-of-line resistors that are 1000 ohm, 1% tolerance.
4. Two output relays support fail-safe and fail-secure operation. One relay shall be used for the strike and is capable of 5A; the other relay may be used for auxiliary functions and is capable of 1A.
5. 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:


2.12 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, is 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:

2.13 CARD READERS

A. The card readers shall be wall-mounted adjacent to the door, on the knob set/handle or opening side. The reader shall be mounted in accordance with current ADA Compliance guidelines.

B. For double door installations, the reader shall be wall-mounted, pedestal mounted or doorframe-mounted on the active leaf side. The inactive door must be monitored with door position switches.

C. All doors must have key override.

D. All-in-one door mounted units are also approved for interior doors not requiring door operators.

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

F. Multi-technology readers must be used and at a minimum must support 125KHz proximity and 13.56 MHz (iClass, MIFARE, DESFire).

2.14 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.

2.15 EGRESS MOTION DETECTORS

A. Use of motion detection for egress is unacceptable without prior approval from CUPD Access Control and the Central Zone Lock Shop.

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.
2.16 MISCELLANEOUS REQUIREMENTS

A. Equipment shall be located 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. Control equipment shall be mounted at a convenient height for future servicing.

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

C. Equipment enclosures shall have locking mechanisms that are left locked and located on the secured side of the system.

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 Division 1, General Requirements.

PART 3: EXECUTION

3.01 SYSTEM PROGRAMMING

A. Cornell’s Central Shops Fire Alarms & Security Technician or a Lenel certified contracted programmer should perform the initial setup programming prior to the installation. A completed “Installation Checklist” for the facility shall be delivered and accepted by the installation’s project and/or construction manager as well as CUPD Access Control’s Program Manager.

B. The building/unit access control coordinator (ACC), for the building implementing the security and access measures, shall supply CUPD Access Control Manager with the information pertaining to the population residing within, and the traffic patterns and times of operation therein.

1. The ACC and their designees will be trained for local management by the security system contractor and CUPD Access Control Manager.
2. ACC authorization forms must be in place prior to this training.

C. The security system installer is responsible for initial alarm programming and commissioning for intrusion devices with approval and collaboration of the Cornell Police Telecommunications and CUPD Crime Prevention.
3.02 TESTING, COMMISSIONING AND ACCEPTANCE

A. 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. The 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.

1. See Cornell CUPD Access Control Consultation/Installation Procedure

B. The CUPD Access Control Project Manager will give a commissioning report to Cornell’s 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.

C. 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 or email via the Unit/College department).

3.03 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.

3.04 PROJECT 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 close out of the project. The Project Manager will ensure these documents are delivered to Cornell’s 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.
Policy documentation:
- Policy 8.1 – Responsible Use of Video Systems
- Policy 8.4 – Management of Keys and Other Access Control Systems

Standards documentation:
- DCS – (#tbd) – Electronic Safety and Security Systems

Required documentation for Installation:
You can find all of the following forms at https://cardaccess.cornell.edu/Documentation/procedures.cfm
- Access Control Activation form
- ACC authorization form
- NVSS authorization form
- NVSS training and Attestation form
- Intrusion system form

What Is University Centralized Access Control?
Everyone acting on behalf of Cornell University must take responsibility for faculty, staff, and student safety, as well as the security of university physical space and the assets contained therein. An essential element of security is maintaining adequate control to ensure that only those authorized to do so access university assets. Although access control systems may vary in different situations, Policies 8.1 and 8.4 promulgate minimum practices that must be maintained throughout the university. It is recognized that certain agencies and units, by nature of their roles and responsibilities at the university, possess some access devices that allow for broad or unrestricted access.

All units using card access, video surveillance or intrusion systems must be integrated with the central campus system. Per policy, any stand-alone system must be specifically exempted through a procedure outlined in each policy. In addition, any unit with an existing stand-alone system will have five years from the promulgation of this policy to convert to the central system or obtain an exemption. Approval for any exemption will be considered by the Chief of Police and Director of Risk Management and Insurance, and will be based upon specific business needs, such as undue hardship.
The Cornell Ithaca Campus, and other non-campus designated locations such as New York City CFEM program and Geneva NY are on the centralized access control system. While the University’s Access Control Program maintains the systems and servers centrally, the management of individual card access and video monitoring is at the local unit level.

**Cornell Standard for Card Access and Video Surveillance: Stanley BASIS System (see CDS 28.10.00)**

- Synchronizes with the registrar’s list of more than 50,000 Cornell Faculty, Staff, and Students every 20 minutes to ensure an up to date and accurate database of active cardholders
- Maintained and supported 24/7 by the Cornell University Police Access Control Program
- The centralized system can be administered (by an authorized user) from any personal computer with Citrix receiver, VPN, and an internet connection
- The system’s software is licensed to the university and the cost to you, as an additional user is minimal, and includes support, licensing, maintenances, updates and upgrades.
- All servers are housed in Rhodes server farm and are monitored.
- Databases are backed up nightly via EZ-Backup to tape and stored redundantly.

**Advantages of ID Card-based locks:**
The card access centralized system uses electronic information pertaining to a particular ID card, which is distributed by the Office of the University Registrar. Authorized personnel monitoring the system can tell who is entering, if the ID used is valid, if the door is held open, or if it was forced open. Decisions about who may enter and who may not are decided by local administrators or building coordinators (referred to as Access Control Coordinators or designee by policy). They program the doors and manage cardholder access assignments.

- **Security:** although not intrinsically a security system, card readers do record the identity of all who attempt entry. They note day and time, whether access was allowed or denied, and whether a valid card was presented. Segment managers may ask the local law enforcement agency, or Cornell Police, to monitor this action as it occurs, thus providing a greater level of accountability and security than what can be attained with ordinary brass locks. Should a higher level of security be required, the central access control group has extensive experience integrating the ID card locks with a traditional intrusion system to create a security system that is both safe and flexible.

- **Cost effectiveness:** Since a support, licensing, and system maintenance structure is already in place at Cornell Ithaca, costs of independent systems are avoided. Additionally you will be supported by a group that is familiar with the systems and Cornell’s practices and procedures with 15 years of combined experience.

Keying and managing the distribution and return of keys can be a significant time sink. Doors with high turnover or need for quick changes can be problematic or impossible to implement with a pure key system. When a key is lost there is also a significant charge to both replace the affected cores but then to also redistribute new keys to your constituents.
• **Ease:** as an authorized user responsible for the card access system, you may enter or change a cardholder’s privileges in seconds, and do this on the campus network using the BASIS or custom-built web tools.

• **Convenience:** A Cornell ID issued to a cardholder can be programmed to be used on both the NYC and Ithaca campuses thus negating the need for carrying several different identification cards.

• **Flexibility:** Card readers are highly programmable, allowing access control users to assign specific access for cardholders based on a robust combination of days and times. The authorized user can also program doors to lock or unlock at specified times such as the beginning and end of the day, enhancing security.

• **Safety:** In case of emergency, all doors on the card access system can be locked or unlocked at once.

**Advantages of Video:**
Cornell University aims to provide a secure environment for members of its community and to protect personal safety and property, assisted by video surveillance systems technology. Such technologies, however, must be used only to meet the university’s critical goals for security, and in a manner that is sensitive to interests of privacy, free assembly, and expression.

• **Security:** In the event of a security incident, video can be crucial in gathering supporting evidence for an active investigation. Additionally, if an emergency is actively occurring, the Cornell Police department can tap into the video to aid in their response to the situation.

• **Response:** Though not typically monitored live, utilizing a video system provides many benefits in response to an incident. With a non-security related incident (broken tool, accident/injury, etc.), video can be instrumental in determining accuracy of the described event and parties involved. It can also identify areas where training and education may be needed.

**Consultation, Installation, Activation and Commissioning Services:**

• **Consultations:** The University’s Access Control team collaborates closely with Facilities Services and or independent security vendors to provide onsite consultations for customers. Usage, practices, and risks will be discussed during consultations to ensure that the unit/department is getting the systems to meet their needs. For larger construction/renovation projects the Access Control team works with project managers and architects to review building designs.

• **Installation and Activation:** The Access Control team works closely with Facilities Services, Project and constructions managers, and security vendors during the construction and installation process to assure that systems are installed and programmed to integrate into the University’s centralized systems within the Cornell Police department. A final test of the respective security and card access equipment and hardware shall be performed prior to considering the installation to be “complete”. In the case of a new building or renovation, this should be done prior to building occupation. The system is not activated (“live”) until documentation is in place. This would include the Activation form, the ACC or NVSS authorization forms, the Intrusion system form, and in the case of video, the NVSS training and Attestation form.
• **Commissioning:** Once the security systems have been installed, the project and/or construction manager will conduct a security systems commissioning with the Access Control Project Manager, the Security Contractor/Installer, and Electrical contractor when applicable. This should be scheduled two weeks prior to the completion of the installation of a tentative testing date. The Access Control Project Manager may include an independent certified electrician as needed in the commissioning. It is the responsibility of the project to fund this resource. On that date, a full system test will be performed encompassing each opening, camera, and alarm point focusing on the following:
  - **Access Control:** verification of credential validation, door position switch functionality, request to exit functionality, and proper door closure
  - **Video:** Recording verification, live data connection, adequate focus, and system owner acceptance of view
  - **Integrated Intrusion Detection:** verification of credential validation, door position switch functionality, request to exit functionality, proper door closure, and validation of alarm signal.

The CUPD Access Control representative 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 test will be tested again. The extent of the retest shall be up to the discretion of Access Control Program Manager.
  - If occupation occurs prior to Access Control commissioning, occupants must be notified of potential security risks.

**The Cost of Centralized Access Control:**
Costs vary depending on the circumstances of the installation. However, if you choose centralized access control, your savings in maintenance could be significant as costs for software, storage, server maintenance and backups are handled centrally with only a basic annual fee per device. This fee also includes 24/7 help request services. In most units using card access, people/time resources will be freed up significantly because student/staff data is updated automatically from PeopleSoft and the system’s capabilities for managing access and door automation will decrease the need for distribution of keys and daily door management. Hardware replacement costs do remain with the unit/department.

• **Initial***:
  - **Wired Card Access** – $5,000 – $9,000/door
  - **Wireless Card Access** - $2,000 - $5,000/ door *(only in approved areas*)
  - **Video System** – $1,000 - $4,000+/camera (camera dependent)
  - **Intrusion** - *(TBD)*

*there may be additional charges for asbestos investigation prior to work start. Contact Facilities Services for additional information

• **Ongoing**
  - **Access Control** - $195/year/panel or reader (FY14 dollars)
    - **Video** - $260/year ($194 + $75 server space (FY14 dollars)
    - **Intrusion** - *(TBD)*

**Ongoing rates reviewed annually**
How do I schedule a consultation or get an estimate?

Consultations and Questions:
- Contact the Access Control Project Manager (5-7874) to schedule a consultation for your unit’s needs
- For Intrusion installation, Communications Manager, CUPD (5-4676)

Estimates
- For new project installations or system additions, you can submit an estimate request to Facilities Services.
- Large construction or renovation projects are most often handled within the construction management and bidding processes.

Questions?
If you have any questions or concerns, or just want to learn more about the program or what is available, please contact us:
- accesscontrol@cornell.edu
- call 255-7874 (ACP Manager)

Attachments:
You can find all of the following forms at https://cardaccess.cornell.edu/Documentation/procedures.cfm
- Access Control Activation form
- ACC authorization form
- NVSS authorization form
- NVSS training and Attestation form
- Intrusion system form