

DIVISION 28 – ELECTRONIC SAFETY & SECURITY

Section Number	Title
28 01 00	Operation and Maintenance of Electronic Safety and Security
28 01 10	Operation and Maintenance of Electronic Access Control Systems
28 01 20	Operation and Maintenance of Electronic Surveillance
28 05 00	Common Work Results for Electronic Safety and Security
28 05 13	Conductors and Cables for Electronic Safety and Security
28 05 26	Grounding and Bonding for Electronic Safety and Security
28 05 28	Pathways for Electronic Safety and Security
28 05 53	Identification for Electronic Safety and Security
28 06 00	Schedules for Electronic Safety and Security
28 06 10	Schedules for Electronic Access Control System
28 06 20	Schedules for Electronic Surveillance
28 08 10	Commissioning of Electronic Safety and Security
28 08 10	Commissioning of Electronic Access Control Systems
28 08 20	Commissioning of Electronic Surveillance
28 13 00	Access Control System
28 13 01	Access Control System Installation
28 13 13	Access Control Global Applications
28 13 16	Access Control Systems and Database Management
28 13 19	Access Control Systems Infrastructure
28 13 26	Access Control Remote Devices
28 13 43	Access Control Identification Management System
28 16 00	Intrusion Detection
28 23 00	Video Surveillance System
28 23 01	Video Surveillance System Installation
28 23 13	Video Surveillance Control and Management System
28 23 19	Digital Video Recording Devices
28 23 23	Video Surveillance Systems Infrastructure
28 23 29	Video Surveillance Remote Devices and Sensors
28 26 00	Electronic Personal Protection System
28 30 00	Electronic Detection and Alarm

Section Title
Number

28 01 00 Operation and Maintenance of Electronic Safety and Security

DESCRIPTION

The operation, oversight and maintenance of all Electronic Access Control and Intrusion Detection Systems, herein referred to as Northern Arizona University’s Physical Access Security System (NAUPASS), is a shared responsibility of the following department/offices:

- 1.) Campus Services and Activities IT
- 2.) Facility Services Access Services
- 3.) Facility Services Planning, Design and Construction
- 4.) Northern Arizona University Police Department.

Individual departments and offices within the University may have access to discreet or combined segments; however, responsibility for access control and intrusion and intrusion detection as a complete University-wide system falls within the purview of the abovementioned departments and the guidance of the University administration. NAUPASS installations under this division shall provide controlled access to building areas, interior and exterior, real-time monitoring of doors at multiple locations simultaneously, local alarms indicating doors have been forced or held-open, and real time and archived security footage as needed.

Prior to commencement of any access system installation by approved contractor, any applicable segment licenses must be requested through Planning, Design and Construction and coordinated with Campus Services and Activities IT.

All material shall comply with the most current applicable sections of the following codes for installation of access control and intrusion detection cabling:

- 1.) International Building Code (IBC)
- 2.) National Electrical Code (NEC/NFPA70/NFPA731)
- 3.) National Electrical Safety Code (NESC IEEE C2)
- 4.) Local codes, amendment and ordinances

All components, installation practices, and final commissioned systems shall maintain compliance with all applicable sections of the International Organization for Standardization (ISO)/ International Electro-technical Commission (IEC) 27002:2005: Information Security Management Code of Practice.

28 01 10 Operation and Maintenance of Electronic Access Control Systems

The electronic access control portion of NAUPASS is a modular and upgradable multi-user, multi-tasking system with granular permissions for control and access that is capable of monitoring, recording and displaying supervised alarm inputs/outputs and reader access activity on a continuous real time basis. All access control panels must have the capability to authorize and verify access and store and manage system activity



Section Title
Number

in both on-line and off-line modes. The panels must operate as standalone units if required for a limited amount of time and automatically download all offline data to the server once reconnected. All control panels must provide for continuous real time polling back to the central processor and must accept firmware updates via network communication. End of line devices will be connected to the field control panels. Any readers connected to access control panels will be polled on a continuous basis to verify connectivity. The operation and maintenance of the Electronic Access Control Systems falls under the authority of NAU’s Campus Services and Activities IT Office (CSA-IT) and Facility Services’ (FS) Access Services. Any and all changes or modifications shall be coordinated with CSA-IT and FS Access Services prior to commencement of activity.

28 01 20 Operation and Maintenance of Electronic Surveillance

The electronic surveillance portion of NAUPASS is a modular and upgradable multi-user system with granular permissions for control and access that is capable of monitoring, recording and displaying images and video from multiple cameras and input devices in a continuous real time basis. The individual electronic surveillance units must operate as standalone units if required for a limited amount of time and automatically download all offline data to the server once reconnected. All surveillance footage storage devices must provide for continuous real time polling back to the central server and must accept updates via network communication. The operation and maintenance of Electronic Surveillance falls under the authority of NAU’s Police Department (NAUPD). Any and all changes or modifications shall be coordinated with CSA-IT and NAUPD prior to commencement of activity.

28 05 00 Common Work Results for Electronic Safety and Security

MINIMUM INSTALL REQUIREMENTS

References to industry and trade association standards and codes are minimum installation requirement standards.

Drawings and other specification as noted in project manuals shall govern in those instances where requirements are greater than those specified in the above standards.

MANUFACTURED PRODUCTS

Materials and equipment furnished shall be of current production by manufacturers regularly engaged in the manufacture of such items, for which replacement parts shall be available. When more than one unit of the same class of equipment is required, such units shall be the product of a single manufacturer. Components shall be compatible with each other and with the total assembly for the intended service.

EQUIPMENT LOCATION

Final equipment installation shall be in a location conducive and appropriate for the installation of sensitive electronic equipment and as close as practical to locations(s) shown on the drawings. If equipment is to be located in a building MDF or IDF, room resign and rack/ component placement must be approved by NAU Information

DIVISION 28 – ELECTRONIC SAFETY & SECURITY

Section Title
Number

Technology Services (NAU ITS). If it is deemed by NAU ITS, Facility Services Planning, Design and Construction (FS PDC) and/ or the Design Professional (DP) that the installed equipment is not located appropriately, or is not conveniently accessible for operation and maintenance, or that the equipment is not installed as designed or notated on the drawings, the equipment shall be removed and reinstalled as directed at no additional cost. All Access Control reader interface modules, reader controllers, or system controllers as well as all Remote Digital Video Recorders must be located in rooms that are secured under the Lenel OnGuard Access Control System as a part of NAUPASS.

MANUFACTURED PRODUCTS

Materials and equipment furnished shall be of current production by manufacturers regularly engaged in the manufacture of such items, for which replacement parts shall be available. When more than one unit of the same class of equipment is required, such units shall be the product of a single manufacturer. Components shall be compatible with each other and with the total assembly for the intended service.

SUBMITTALS

- a.) In cases of new construction where installer will necessarily coordinate with a general contractor and design professional, installer shall furnish the following literature and data showing all individual component type and rating and full equipment manufacturer datasheets to FS PDC or GC/CMAR as appropriate:
 1. Product data for all equipment, hardware cabling and miscellaneous components proposed.
 2. Floor plan drawings showing equipment and device locations with proposed conduit, wiring, pull box and junction box locations
 3. Camera mounting details specific to location
 4. Schematic or One-Line drawings – dependent on specific project - of all circuits from the field devices to the required connection points. The diagrams shall show wiring of equipment and all connections to be made to devices. Terminal connections in the equipment shall be numbered to correspond to the diagrams for use in making connections. Wiring diagrams shall be coordinated so that terminal numbering, circuit designation and equipment or device designations are the same on all drawings and coordinated per 28 05 53. All drawings must be submitted and approved by the Engineer before installation starts, but such approval will not waive any specification requirements unless specifically stated
- b.) In cases of individual or standalone electronic safety and security installations, installer shall furnish FS PDC with the above listed literature and data showing each individual component type and rating and full manufacturer equipment datasheets. All submittals furnished to FS PDC shall indicate clearly any variances from original project design documents.
- c.) Mark submittal package with specification section number. Do not mix sections

Section Title
Number

- in a single submittal.
- d.) Mark general catalog sheets and drawings to indicate specific items being submitted and proper identification of equipment by name and/or number, as indicated in the contract documents.
 - a. Markings shall be reproducible (arrow, underlines, circled, checkmark, etc.).
 - b. Where sheet or drawing includes options, mark proposed option(s).
 - c. When manufacturer's reference numbers are different from those specified, provide explanation and cross-reference number for each item.
 - e.) Work shall not proceed without NAU and consultants approval of the submitted item.
 - f.) No substituted materials shall be installed except by written approval from FS PDC.
 - g.) The Owner reserves the right to make changes to descriptive information, component selection and nomenclature during shop drawing review without incurring any additional cost.

EQUIPMENT REQUIREMENTS

Where a variation in equipment or materials is requested from the original approved design drawings, construction documents, or materials quote in accordance with General Conditions 2.5.13.5 SUBMITTALS DRAWINGS, AND SHOP DRAWINGS, it is the responsibility of the installer to coordinate work and guarantee compatibility with existing equipment, designed equipment, and any other impacted trades.

OUTAGES

No outages shall be permitted on existing systems except at the time and during the interval specified by NAU and site representatives. The site may require written approval.

Any outage must be scheduled when the interruption causes the least interference with normal site schedules and business routines. No extra costs will be paid to the Contractor for such outages which must occur outside of regular weekly working hours. Integrator shall restore any circuit interrupted as a result of this work to proper operation as soon as possible.

28 05 13 Conductors and Cables for Electronic Safety and Security

DESCRIPTION

This section specifies the furnishing, installation, and connection of the conductors and cables for electronic safety and security.

RELATED WORK

- a.) Sealing around penetrations to maintain the integrity of time rated construction: Section 10523, FIRE STOPPING.
- b.) General electrical requirements as related to multiple areas: Division 26: 26 00



DIVISION 28 – ELECTRONIC SAFETY & SECURITY

Section Title
Number

00 ELECTRICAL SERVICES

- c.) Conduits for cables and wiring: Division 26: 26 05 33 RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS; Division 27: 27.05.28 PATHWAYS FOR COMMUNICATION SYSTEMS
- d.) Requirements for personnel safety and to provide a low impedance path for possible ground fault currents: Section 26 05 26 GROUND FAULT PROTECTION SYSTEMS, GROUNDING AND BONDING
- e.) Power conditioning on system controller boards and door controller boards shall meet minimum requirements: Division 26.
- f.) Requirements for Electronic Safety and Security IP Based Communication Conductors and Cabling: Division 27: 27.10.00 STRUCTURED CABLING.

ACCESS CONTROL LINE VOLTAGE AND CONTROL WIRING

- a.) Unless otherwise specified in other sections of these specifications, line voltage wiring shall be as specified by the manufacturer, except the minimum size shall be not less than No. 12 AWG.
- b.) Unless otherwise specified in other sections of these specifications, control wiring, either 12 or 24V DC, shall be as specified by the manufacturer, except the minimum size shall be not less than No. 14 AWG
- c.) Wiring shall be large enough so that the voltage drop under inrush conditions does not adversely affect operation of the supplied equipment or initiate a battery back-up power condition.

ACCESS CONTROL COMMUNICATION CONDUCTORS AND CABLE (NON-IP BASED)

28.05.13.16

- a.) Shall at minimum conform to the recommendations of the manufacturers of the communication and signal system. In the event that communication or signal wiring is related to other divisions and sections in this specification, whichever is greater shall be primary.
- b.) All cable shall be UL listed.
- c.) Cable shall be plenum rated unless specifically designated
- d.) Multi-conductor cables shall have the conductors color coded.

28 05 26 Grounding and Bonding for Electronic Safety and Security

DESCRIPTION

All conductors used for grounding will be color coded green continuously in all visible places, cabinets, equipment, pull boxes, junction boxes, switchboards, etc., or shall be bare copper continuously. Conductors used for isolated grounds shall be green with orange stripe or tracer.

RELATED WORK

- a.) Requirements for live level voltage equipment grounding: Division 26: 26 05 26 GROUNDING AND BONDING FOR ELECTRICAL SYSTEMS.
- b.) Requirements for low-voltage and communication system grounding: Division

Section Title
Number

27: 27.05.26 GROUNDING AND BONDING FOR COMMUNICATION SYSTEMS

28 05 28 Pathways for Electronic Safety and Security

DESCRIPTION

This section specifies the physical routes and pathways allowable for conductors and cables for electronic safety and security as well as appropriate methodology to install cable along these pathways. All wall and floor penetrations shall be sleeved and fire stopped as required. IP-based communication cabling used in Electronic Safety and Security may share common pathways with Division 28 Voice/data Communication cable as long as all applicable identification protocols are followed and shared cable trays/ pathways meet sizing requirements of Division 28 inclusive of all Division 27 and 28 cables.

RELATED WORK

- a.) Requirements for IP-based Electronic Safety and Security hangers and support: Division 27: 27.05.28.29 HANGERS AND SUPPORT FOR COMMUNICATION SYSTEMS
- b.) Requirements for IP-based Electronic Safety and Security conduits and back boxes: Division 27: 27.05.28.33 CONDUITS AND BACK BOXES FOR COMMUNICATION SYSTEMS
- c.) Requirements for IP-based Electronic Safety and Security cable trays: Division 27: 27.05.28.36: CABLE TRAYS FOR COMMUNICATION SYSTEMS
- d.) Requirements for IP-based Electronic Safety and Security surface raceways: Division 27: 27.05.28.39 SURFACE RACEWAYS FOR COMMUNICATION SYSTEMS

TERMINATIONS, SPLICES AND CONNECTIONS 28.05.28.13

- a.) Installer shall splice or otherwise connect cables and wires only in termination back-boxes, junction boxes, or pull boxes.
- b.) Boxes designated for existing voice/data pathways may not be utilized
- c.) Cover plates for boxes shall conform to Division 26.
- d.) Splices, terminations, and connections shall be mechanically and electrically secure.

HANGERS AND SUPPORT FOR ELECTRONIC ACCESS AND SECURITY 28 05 28.29

- a.) Cabling run in plenum spaces shall be self-supported with J-hooks either from the wall or from deck supported hanger wire.
- b.) IP-based communication cable may share J-hooks and cable trays with voice/data cable runs as long as there is an approved physical separation between cable types.

CONDUITS AND BACKBOXES FOR ELECTRONIC SAFETY AND SECURITY 28 05 28.33

- a.) Cabling through areas accessible to the public that cannot be routed through plenum space or interior wall must be run in rigid steel or other form of surface

Section Title
Number

- mounted conduit.
- b.) Minimum conduit size of ¾ inch, but not less than the size shown on the drawings.
- c.) All conduit ends shall be equipped with insulated bushings.
- d.) Control wire from the power supply transformer to the door actuator may not share any pathway, conduit, junction box, or backbox with data/voice or communication/signal wire.
- e.) All control wire pathways shall maintain a minimum distance of 12 inches away from any data/voice communication runs.

CABLE PULLING

- a.) Installer shall provide and utilize equipment that will prevent the cutting or abrasion of insulation during pulling of cables.
- b.) Installer shall use ropes made of nonmetallic material for pulling feeders.
- c.) Installer shall attach pulling lines for feeders by means of either woven basket grips or pulling eyes attached directly to the conductors.
- d.) Installer shall pull in multiple cables together in a single conduit.
- e.) Any compound or product used shall be suitable for the wire insulation and conduit it is used with and shall not harden or become adhesive after use.

EXISTING WIRING

Unless specifically indicated on the plans, existing wiring shall not be reused for the new installation. Only wiring that conforms to the specifications and applicable codes may be reused. If existing wiring does not meet these requirements, existing wiring may not be reused and new wires shall be installed.

28 05 53 Identification for Electronic Safety and Security

EQUIPMENT IDENTIFICATION

Any enclosures for access control interface boards or other auxiliary control units that are not located immediately adjacent to or above the door or area that they are associated with must indicate all pertinent information required for maintenance or repair of equipment including the connected door or area and assigned NAUPASS software identification label.

CONTROL, COMMUNICATION AND SIGNAL SYSTEM IDENTIFICATION

- a.) IP-Based Communication cable must follow Division 27: 27.10.00 STRUCTURED CABLING color codes in addition to all other specified Division 28 identification protocols.
- b.) Installer shall place a permanent wire marker on each wire at each termination point in order to allow identification of wire source and destination.
- c.) Permanent wire marker shall correspond to notations on wiring diagrams or as-built construction documents used for installation the system
- d.) Installer shall place a label or otherwise denote the wiring schedule for all

Section Title
Number

- terminations of color-coded multi-conductor signal cable. Wire marking is not necessary on individual conductors; however, a schedule of conductors must be visible on the piece of equipment or mounting box.
- e.) Identifying colors on the multi-conductor wire schedules shall correspond to those on the wiring diagrams or as-built construction documents used for installation the system.
 - f.) Wire markers shall retain their markings after cleaning.

28 06 00 Schedules for Electronic Safety and Security

The following network configurations will be required for all network components which will integrate/interface with NAUPASS. Each component shall have its MAC address registered through the University’s Dynamic Name Service (DNS) to use a fixed DHCP address appropriate to the building or facility subnet. Devices that are required to register addresses and utilize the following network conventions include but are not limited to: intelligent system controllers, intelligent reader controllers, IP surveillance cameras, and Digital Video Recorders. Individual subnets, MAC Address registration, and Fixed-DHCP IP addresses shall be coordinated with ITS Network Operations Center (NOC). All Devices unless otherwise called for, shall use a private address

IP Subnet Table		
	Public IP Subnet	134.114.x.x
	Private IP Subnet	10.x.x.x
	Secure Wireless Subnet	10.18.x.x

All network components which will integrate/interface with NAUPASS and are assigned IP addresses on the NAU network according to the above table will also be required to have a network Hostname assigned that follows the following naming conventions:

- LNL-{BuildingNumber}-{Device Type}{DeviceNumber}.ss.nau.edu
- (e.g.: LNL-30-DVR1.ss.nau.edu)

Reference appropriate Building Numbers for facilities on the NAU Campus at:
<http://www.nau.edu/postal/BuildingAddresses/>

Section Title
Number

Device Type Abbreviation Table	
Digital Video Recorder	DVR
IP Video Camera	CAM
3300 Intelligent System Controller	3300PNL
LNL500W Wireless Intelligent System Controller	500WPNL
LNL2200 Intelligent System Controller	2200PNL

28 06 10 Schedules for Access Control

DESCRIPTION

The following schedules and diagrams may serve as a guide for items common to multiple titles in Division 28 but shall serve specifically for Access Control. Additional equipment may be installed with appropriate approval and substitutions may be made as long as all substituted product models are approved by Campus Services and Activities IT, FS PDC, and FS Access Services.

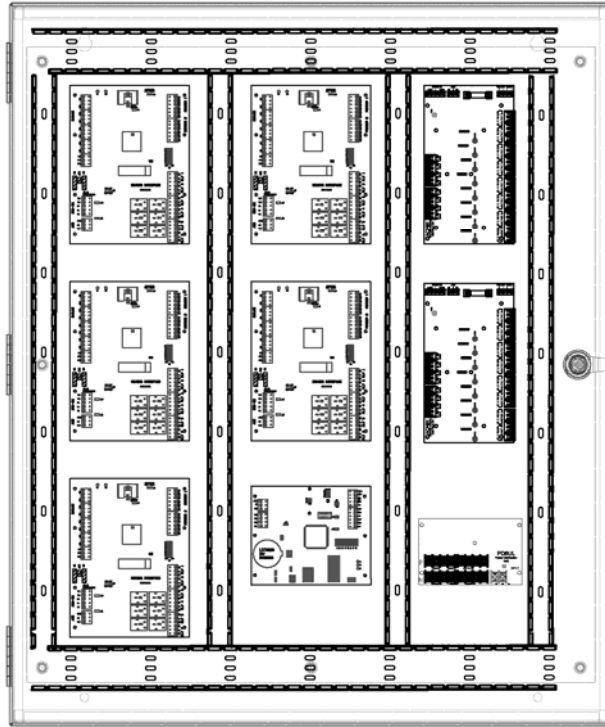
Integrator is responsible for altering or upgrading any stated equipment model numbers due to manufacturer product model number changes, obsolescence or equipment design.

Integrator shall provide equipment suitable for the capacities indicated in the construction documents. Any discrepancies in quantities shall include the greater quantity in Integrator's proposal.

Quantities listed in the construction documents are to provide location information to the bidding contractors. Integrator shall be responsible for identifying and verifying all equipment quantities and actual placements of devices. The NAU representatives shall not be responsible for any discrepancies in the quantities of equipment.

Section
Number Title

Typical System and Door Controller Panel Enclosure
With Fused Power Distribution

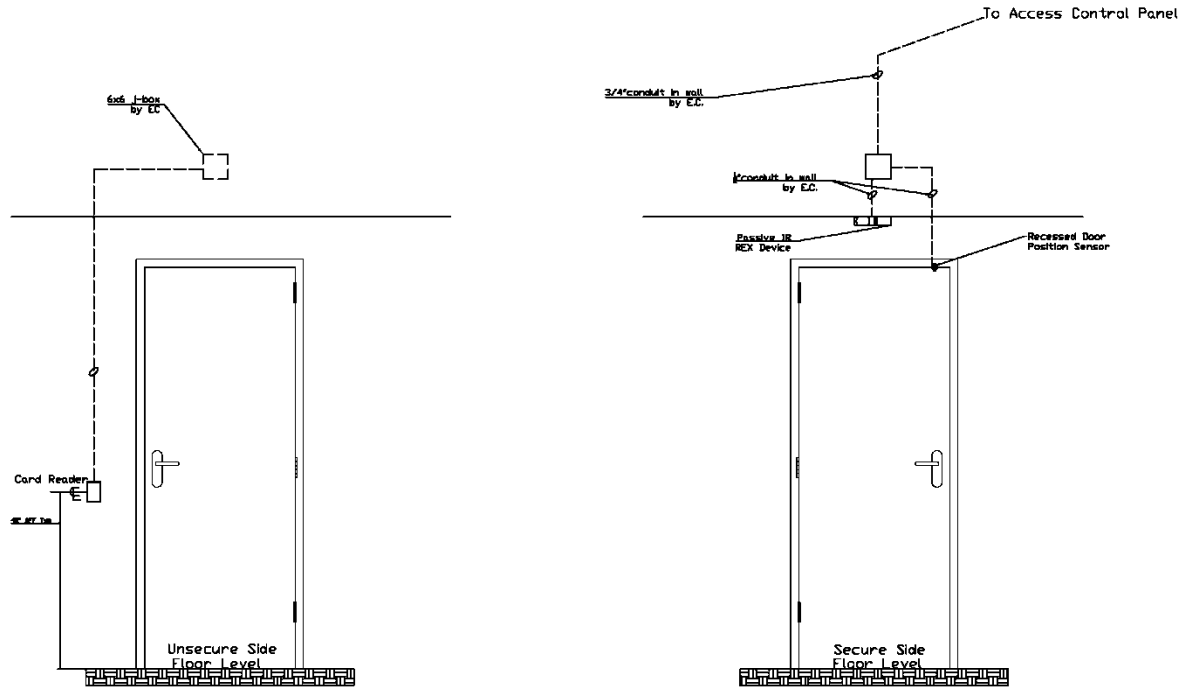


FIELD EQUIPMENT

1	Hoffman	A36N30ALP	36x30 Enclosure
1	Hoffman	A36N30MP	Back Panel
1	Hoffman	A-L12AR	Cylinder Lock Kit
1	GRI	PB2020-T	3/8" Tamper Switch
12'	Panduit	G1X2WH6	1" Panduit
12'	Panduit	C1WH6	1" Cover
6'	Panduit	G15X2WH6	1.5" Panduit
6'	Panduit	C15WH6	1.5" Cover
1	Altronix	MAXIMAL75E	12V 10A + 24V 10A Power Supply (Not Shown)
2	Altronix	ACM8CB	Access Power Controller
1	Altronix	PD8UL	Power Distribution Board
3	Yuasa (or equivalent)	NP712	12Vdc, 7Ah Battery (Not Shown)

Section Title
Number

Typical Single Door with Electrified Handset or Strike



FIELD EQUIPMENT

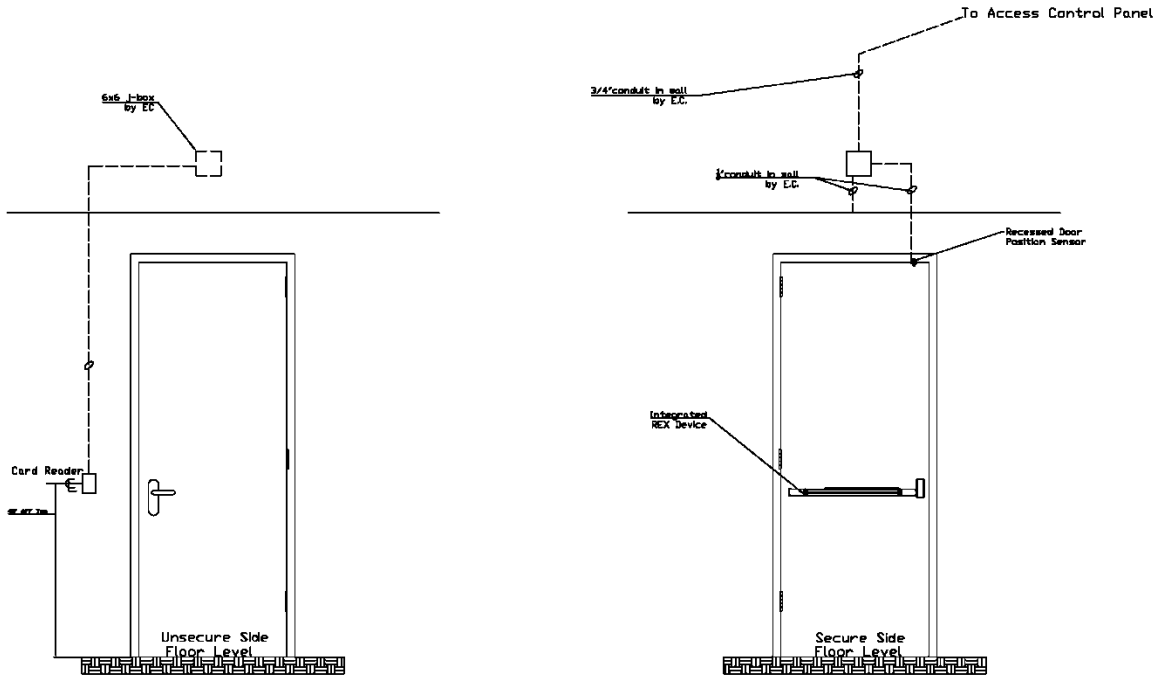
Card Reader	HID	MultiCLASS SE RP40
Electrified handset or Strike		See Division 8
Passive IR Request to Exit Device	Bosch	DS160 (Light gray w/ sounder)
Recessed Door Position Sensor	GRI	180-12 (3/4" Gray in color)
Controller to REX connection	Belden or Equivalent	AWG 22/6 CMP 6504UE
Controller to DPS connection	Belden or Equivalent	AWG 22/4 CMP 6502UE
Controller to Card Reader connection	Belden or Equivalent	AWG 22/6 CMP 6504FE

Note:

- Automatic Door Closer to be provided and installed by others but integrated in to the Electronic Safety and Security System by Division 28 Integrator.

Section Title
Number

Typical Single Door with Exit Bar with built-in Request to Exit Device



FIELD EQUIPMENT

Card Reader	HID	MultiCLASS SE RP40
Electrified handset or Strike		See Division 8
Passive IR Request to Exit Device	Bosch	DS160 (Light gray w/ sounder)
Recessed Door Position Sensor	GRI	180-12 (3/4" Gray in color)
Controller to REX connection	Belden or Equivalent	AWG 22/6 CMP 6504UE
Controller to DPS connection	Belden or Equivalent	AWG 22/4 CMP 6502UE
Controller to Card Reader connection	Belden or Equivalent	AWG 22/6 CMP 6504FE

Note:

- Automatic Door Closer to be provided and installed by others but integrated in to the Electronic Safety and Security System by Division 28 Integrator.

Section Title
Number

28 06 20 Schedules for Electronic Surveillance

DESCRIPTION

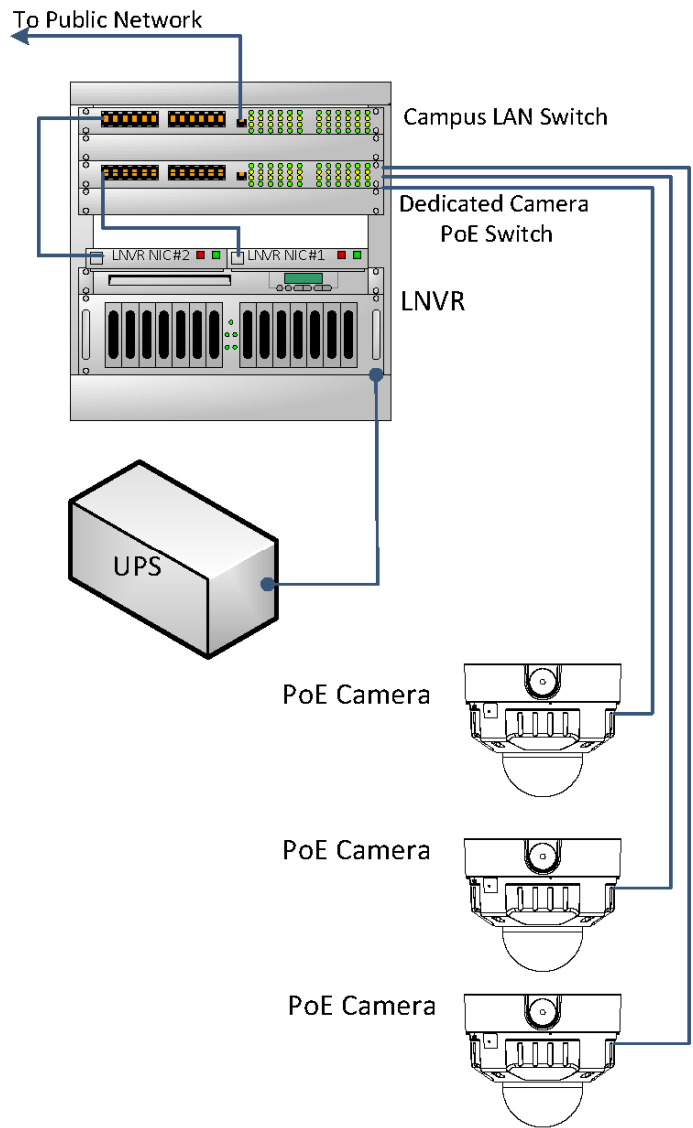
Additional equipment may be installed with appropriate approval and substitutions may be made as long as all substituted product models are approved by appropriate NAUPASS Departments: Campus Services and Activities IT, Facility Services Planning, Design and Construction, and Facility Services Access Services.

Integrator is responsible for altering or upgrading any stated equipment model numbers due to manufacturer product model number changes, obsolescence or equipment design.

Integrator shall provide equipment suitable for the capacities indicated in the construction documents. Any discrepancies in quantities shall include the greater quantity in Integrator's proposal.

Quantities listed in the construction documents are to provide location information to the bidding contractors. Integrator shall be responsible for identifying and verifying all equipment quantities and actual placements of devices. The NAU representatives shall not be responsible for any discrepancies in the quantities of equipment.

Section Number Title



28 08 00 Commissioning of Electronic Safety and Security

DESCRIPTION

Commissioning of Electronic Safety and Security equipment requires the use of Notice of Substantial Completion form (FS-81) held by the assigned FS PDC Project Manager. Upon full execution of the Notice of Substantial Completion, warranty of equipment and installation shall take effect for a period of not less than two years. Commissioning of Electronic Safety and Security systems must meet stated requirements of the facility manager and conform to requirements specified in the individual applicable Division 28 sections. Any access to the System Architecture or Data Communication infrastructure requires that vendors apply for and secure Affiliate Status with the University. Additionally commissioning shall not be considered to be complete until deliverables

Section Title
Number

listed in this document are transferred to the owner(s) and appropriate entities specified in the following section requirements:

SUBSTANTIAL COMPLETION REQUIREMENTS

- a.) Current university version of On Guard client software must be installed on designated owner computer(s).
- b.) Minimum of two hours of training on use of client software shall be provided by installer.
- c.) All licenses must be verified to have been implemented and functioning properly by systems Administrators (Campus Services and Activities IT).
- d.) All equipment, including cable ends must be clearly labeled per 28 05 53.
- e.) All system Door Controller and System Board Controller components installed must be properly identified in the On Guard system software according to schema established by Campus Services and Activities IT.
- f.) All readers must have indicator lights illuminated indicating online or active status and have correct indicator lights and sounds functioning consistently.
- g.) All Access levels created for testing must be removed, and at least one access level must be created, tested and verified to be working to the satisfaction of the owner.
- h.) All default manufacturer and vendor provided passwords for both hardware and software components must be changed and transferred to CSA-IT
- i.) All door hardware components will be operating correctly and according to facility owner expectations.
- j.) Installer will demonstrate successful recording of door activity through alarm monitoring and through system’s reporting functionality.
- k.) All components shall be inspected to ensure they have been properly installed, securely attached, and remain clean, unmarred and are fully operational to the satisfaction of the facility owner.
- l.) All broken, damaged or modified items such as walls, doorframes, ceiling tiles, etc., shall be replaced or properly repaired to the satisfaction of the owner.

DELIVERABLES

- a.) Three (3) final marked as-built record drawings shall be provided by the installer. These shall be delivered grouped with the construction as-builts from the GC if applicable to the project. Copies shall be distributed to the facility owner, CSA-IT, and FS PDC.
- b.) Three (3) sets of individual factory issued Equipment Operations and Manuals containing all technical information on each piece of equipment. Copies shall be distributed to the facility owner, Campus Services and Activities IT, and FS PDC.
- c.) One electronic compiled version of record drawings and O&M documentation shall be delivered to CSA-IT in addition to the printed sets of each.
- d.) A complete schedule of all system components listing:

Section Title
Number

- 1.) Final assigned IP address
 - 2.) Final assigned Host Name
 - 3.) Hardware serial number
 - 4.) Hardware MAC Address
- e.) A complete schedule of all system components noting their installed locations and any variance in equipment from original specification must be included and an approved Technical Standards Variance Request Form should be included.
 - f.) All extra or spare materials shall be delivered and stored on the premises, as directed.
 - g.) A test report of all system components shall be completed and available for inspection by NAU FS PDC, facility owner, Campus Services and Activities IT.
 - h.) Summary document detailing contents of any Vendor provided license files necessary to accommodate additional Lenel components installed on application server. This file(s) will be tested and installed by the University and shall be comprehensive and list separately all existing components as well as new components as part of the project.

WARRANTY

- a.) The system warranty shall be for twenty-four (24) months from the date of substantial completion. Provide all equipment, material, and labor required to uphold a full system warranty at no charge to the Owner. All manufacturers' equipment warranties shall be activated in the Owner's name and shall commence on the date of substantial completion. In the case of modified equipment, the manufacturer's warranty is normally voided. In such cases, provide the Owner with a warranty equivalent to that of the original manufacturer.
- b.) There shall be no cost to the Owner for maintenance performed during the warranty period beyond the fixed cost of the contract.
- c.) Provide a service telephone number, staffed by a qualified technician familiar with the equipment installed. Staff this number during normal business hours.
- d.) Respond with an on-site technician within 6-hours of a service call (including Saturdays and Sundays) for all equipment and system failures.
- e.) Replace or repair, at no cost to the owner, any failed equipment hardware or software installations required to provide full system operations within 48 hours.
- f.) During the warranty period, advise the Owner in writing each time any routine software firmware updates become available, giving the Owner the opportunity to upgrade the software/hardware should they so desire at no additional cost.

28 08 10 Commissioning of Electronic Access Control Systems

After all terminations are completed and network components are installed by either Integrator or Others, Integrator shall conduct a final inspection and pre-test all equipment and system features required for project prior to final acceptance of the Electronic Access Control System and shall perform the following tests at a time

Section Title
Number

mutually agreeable to both a General Contractor representative (if applicable) and an NAU representative from Facility Services PDC and/or CSA-IT. Integrator shall correct any deficiencies discovered as the result of the inspection prior to receiving final acceptance. Integrator may be required to remove covers, open wiring connections, operate equipment, and perform other reasonable work as requested by NAU FS PDC or CSA-IT.

At each installed point of Electronic Access Control the Integrator shall:

- 1) Demonstrate that the installed Card Reader is reading, converting, and transmitting card data back to the reader interface module correctly.
- 2) Demonstrate that the assigned interface module is communicating back to the intelligent system controller (if applicable) and passing the card information through to the Lenel OnGuard Server in Alarm Monitoring.
- 3) Demonstrate that the Lenel OnGuard server has appropriate segmentation, access levels, timezones, and that the test card credential initiates the proper outputs
- 4) Demonstrate that the reader interface board or intelligent system controller operates the appropriate output relays in response to the presented card.

28 08 20 Commissioning of Electronic Surveillance

Integrator shall be responsible for performing the following tests prior to final acceptance of the Video Surveillance System and shall perform these tests at a time mutually agreeable to both a General Contractor representative (if applicable) and an NAU representative from Facility Services PDC and/or CSA-IT:

- 1) Verify the following for each Camera
 - a. Camera produces a clear picture and is aimed per site requirements.
 - b. Camera maintains a clear picture and automatically compensates for changing light conditions including day/night change.
 - c. Camera has wide dynamic range installed where specified and operate to prevent camera blinding
 - d. Camera provides complete and correct coverage of the area specified.
 - e. Cameras are fitted with anti-tamper/ anti-vandalism devices where specified.
 - f. Simulated tamper alarm is transmitted to the operator workstation.
 - g. Functioning of Alarms Input(s)/Output(s) and/or connections to other systems as specified.
 - h. Camera resolution and encoding settings are configured per minimum requirements (28 23 13) and/or as specified per project documents.
- 2) Verify the following for Operator Workstation:
 - a. Display orientation/position, camera/view identification.
 - b. Display and/or notification of alarm condition (if applicable).
 - c. Manual control of cameras (if applicable).
- 3) Verify the following for Recording and Playback Functions:
 - a. Data storage capacity has been installed on the workstation as specified.
 - b. System hardware supplied is per specification.

Section Number	Title
	<ul style="list-style-type: none"> c. Correct video data is recorded by the system in response to simulated alarms. d. Manual Record function operates correctly. e. Playback functions operate correctly including Play, Stop, Pause, Rewind, Fast Forward, Frame by frame view. f. Retrieval of stored video. g. Export of stored video.

Integrator shall be responsible for retaining copies of test results for inclusion in documentation at project completion.

28 13 00 Access Control System

DESCRIPTION

The NAUPASS Access Control component consists of items including but not limited to: cabling, network devices, Lenel System Controllers, Lenel Reader Interfaces, HID Readers, Lenel software clients, Lenel credential design and printing software, and Lenel access control servers. NAUPASS Access Control uses Lenel’s OnGuard Integrated Security Solution for Door Access and Credential Management. All servers and software associated with NAUPASS are administered by Campus Services and Activities Administration.

28 13 01 Access Control System Installation

DESCRIPTION

The integrator/ subcontractor for this scope will be responsible for procurement and installation of a complete Access Control System including: all electronic components generally considered to be directly related access control, integration of this system with the existing NAUPASS, and procurement and transfer of all applicable Lenel license files for University install. Some of these components will be specified under Division 8 Openings. This shall include hardware attached to the door system or any elements adjacent to the door opening that provide input or receive outputs from the door access system (wired or wireless). Installation details shall be clarified on a project by project basis with the General Contractor, if applicable, and Facility Services PDC.

INSTALLER REQUIREMENTS

Integrator must be an approved Lenel Value Added Reseller. Integrator must be established as, or must obtain status as, VAR of record for Northern Arizona University in order to purchase Lenel licensing on behalf of the University. Installation of materials and equipment specified under Division 28 must be completed by a Lenel Certified Technician. Any access to the System Architecture or Data Communication infrastructure of NAUPASS requires that vendor apply for and secure Affiliate Status with the University. The assigned Project Manager shall at a minimum be an affiliate for this purpose along with the installer if appropriate based on size and scope. For additional information regarding affiliate status, visit:

<http://www4.nau.edu/louie/affiliation.html>.



Section Title
Number

PROJECT MANAGEMENT

Integrator shall provide a Project Manager who is experienced in the administration and supervision of the security field and electrical work, both within the various types of security integration and with relation to other types of work and who is hereby authorized to act on behalf of Integrator. The project manager responsibilities will include but are not limited to providing schedules, attending project meetings, submittals, safety, quality control, and testing, training and as-built documentation. The project manager must be an employee of Integrator and working in the security field

28 13 13 Access Control Global Applications

DESCRIPTION

Access control systems are used on campus for the following applications/purposes:

- a.) To restrict physical access to facilities or other resources through the use of approved electronic access control components connected to NAUPASS including physical separation between multiple departments/operating units in a single facility.
- b.) To monitor and/or respond to events including intrusions and irregular door statuses through detection monitored by NAUPD and individual department/system segments.
- c.) To provide reports and audit information for use in investigations by authorized entities
- d.) To manage, identity, and provide access to NAUPASS through central production and issuance of identification cards.
- e.) To create and implement schedules and access levels in order to manage physical access to facilities or other resources
- f.) To record time and attendance in academic classrooms in accordance with University Policy.
- g.) To assign privileges to card holders allowing access to special events, or university resources (ie: Athletic Events, After Hours, and Recreation Facilities).
- h.) Visual verification of identity.

28 13 16 Access Control Systems and Database Management

DESCRIPTION

NAUPASS is managed by a hierarchy of users with NAU Campus Services and Activities IT serving as the top level systems administrator. Individual departments, buildings, facilities or other entities wishing to utilize any component of the NAUPASS system in their area will be required to have a dedicated “Segment Administrator.” Data communications between client computers, servers, and components shall occur on the campus data network infrastructure which is maintained by NAU ITS’s Network Operations Center.



Section Title
Number

SYSTEM ADMINISTRATION

Campus Services and Activities IT shall be responsible for the following:

- a.) Assist in establishing necessary initial access for installers for testing purposes and/or building owner and their designated Segment Administrator(s).
- b.) Coordinate the expansion of the existing NAUPASS system to include installation or implementation of the following devices or resources into the system at a software or programmatic level:
 - Additional System Segments.
 - Alarm Monitoring Zones.
 - System Roles.
 - User Accounts.
 - System Devices such as: DVRs, cameras, door controllers, system boards/controllers/intelligent system controllers etc.
 - Licenses:
 - Door Licenses: May be required to be purchased for each additional door added to the NAUPASS system.
 - Client Licenses: May be required to be purchased for each end user designated to interface with the NAUPASS system.
 - Software Licenses: If the usage of components not already installed on the NAUPASS system is required, coordination and consultation with the Dining and Card IT office is required before purchase of the license. DACA IT reserves the right to review, test and if necessary, reject any code, script or custom software intended to interface in any way with the NAUPASS system for ANY purpose.
 - Cross Segment Access assignment must be authorized by NAUPD or Facility Services at the director level or higher and facilitated through DACA IT.

SEGMENT ADMINISTRATION

Segment Administrator(s) shall be responsible for the following:

- a.) Creating access levels for facilities, doors, or other resources through the On Guard System.
- b.) Assigning access levels inclusive of:
 - Schedules (including Holiday Schedules) – When the door/resource is able to be accessed
 - Doors – Which resource or entrance/exit passages are included.
 - Cardholders – To whom access levels are assigned.
- c.) Removing access from persons no longer affiliated or requiring access.
- d.) Providing additional personnel access to the NAUPASS system.
- e.) Creating Roles within the NAUPASS system to assign to end users within the segment.
- f.) Creating Alarms based on specific events (IF NAUPD is to be alerted of certain events then coordination with NAUPD must be established).
- g.) Obtaining training for usage of the system from Dining and Card Admin IT,

Section Title
Number

through access to user groups, documentation and other available resources.

DATABASE MANAGEMENT

Direct access to any database used with the NAUPASS system is restricted to DACA authorized personnel only. Any request for access to servers containing the NAUPASS database must be submitted in writing to the office of CSA IT, and may require additional administrative approval before such access is granted. Requests must contain contact information, and a detailed explanation of the purpose for the request. NAUPASS Video Surveillance Systems consists of items including, but not limited to: cabling, network devices, Lenel Network Video Recorders (LNVR), client workstations, connectors, client software licenses, and documentation.

SERVERS

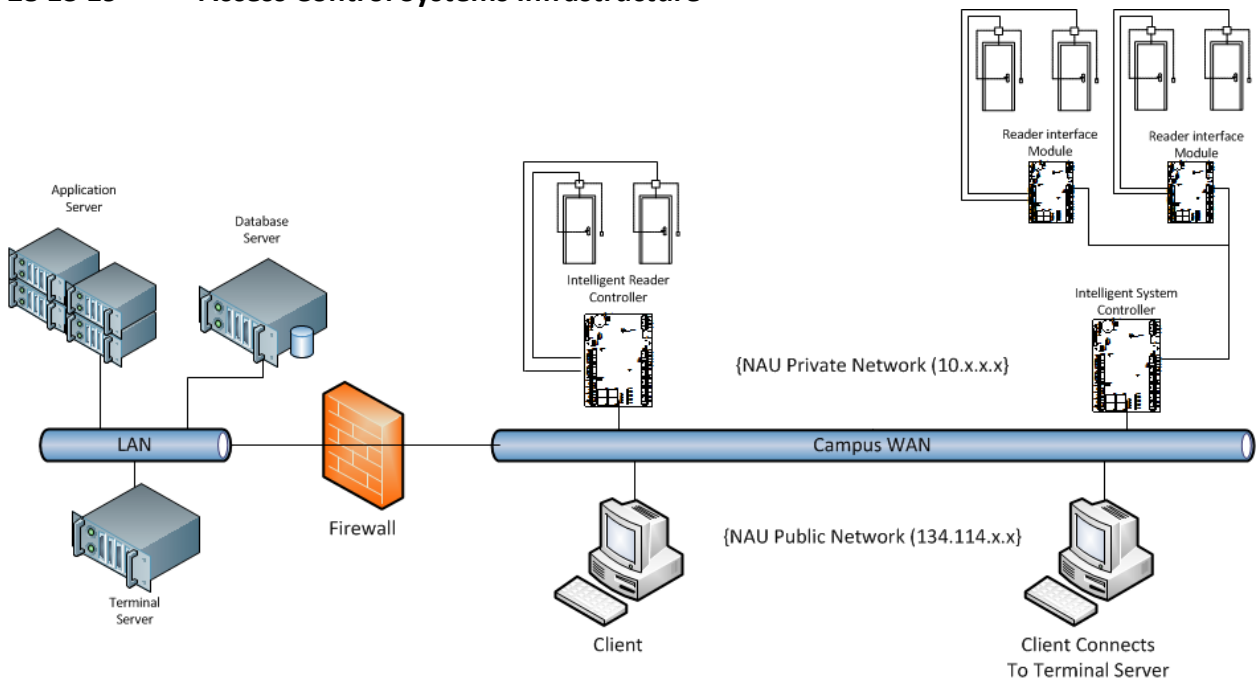
NAUPASS servers are maintained in Hyper V (Microsoft) Cluster. Campus Services and Activities IT also maintains a “test” server used for development purposes (LNLTEST). Access to any of the servers requires authorization by Campus Services and Activities IT. Any implementations of Door Access MUST utilize existing NAUPASS servers. New servers are not permitted and door access systems may not be managed or implemented independent of the established, existing infrastructure except in special circumstances where prior approval has been obtained from either the NAUPASS committee, or from the Office of the President.

Servers to be used with the NAUPASS system will:

- a.) Have a comprehensive Back up and disaster recovery plan.
- b.) Be housed in accordance with applicable standards.
- c.) Have a primary system application/database server to be housed within Co-Location facility which shall have:
 - Back up emergency power.
 - 24/7/365 access available to authorized Campus Services and Activities IT personnel.
 - FM-200 waterless fire suppression or equal protection certified by the NAU Fire Marshall
 - Restricted and monitored physical access

Section Number
28 13 19

Title
Access Control Systems Infrastructure



28 13 26 Access Control Remote Devices

The following equipment is a list of access control remote equipment that is approved for installation on campus:

- Lenel 1320 Dual Reader Interface Module
- Lenel 2210 Intelligent Single Reader Controller
- Lenel 2220 Intelligent Dual Reader Controller
- Lenel 3300 Intelligent System Controller
- HID multiCLASS SE RP40
- HID multiCLASS SE RPK40

28 13 43 Access Control Identification Management System

Cards or credentials issued by the NAU Jacks Card Office are acceptable credentials used for interfacing with the NAUPASS system. All other cards, fobs, RFID, electronic devices, or magnetically encoded devices are strictly prohibited.

28 16 00 Intrusion Detection

DESCRIPTION

Intrusion detection systems including burglary and/or perimeter protection systems are not currently a component of NAUPASS. Reporting and communications for individual installations must be coordinated directly with NAUPD for monitoring and response.

Section Title
Number

28 23 00 Video Surveillance System

DESCRIPTION

NAUPASS Video Surveillance Systems consists of items including, but not limited to: cabling, network devices, Lenel Network Video Recorders (LNVR's), client workstations, client software licenses, and documentation. NAUPASS Video Surveillance uses Lenel's OnGuard Integrated Security Solution to interface with the electronic video monitoring system. All servers and software associated with NAUPASS are administered by Campus Services and Activities Administration. NAUPASS Video Surveillance System's architecture consists of decentralized network digital video recorders that are managed by separate segment administrators on campus. Data communications between client computers, servers, and components shall occur on the campus data network infrastructure which is maintained by NAU Information Technology Services Network Operations Center.

28 23 01 Video Surveillance System Installation

DESCRIPTION

The integrator / subcontractor for this scope will be responsible for procurement and installation of a complete video surveillance system including all electronic components generally considered to be directly related to video surveillance including: integration of this system with the existing NAUPASS and procurement and transfer of all applicable Lenel license files for University install. Installation details shall be clarified on a project by project basis with the General Contractor, if applicable, and Facility Services PDC.

INSTALLER REQUIREMENTS

Integrator must be an approved Lenel Value Added Reseller. Integrator must be established, or must obtain status, as VAR of record for Northern Arizona University in order to purchase Lenel licensing on behalf of the University. Installation of materials and equipment specified under Division 28 must be completed by a Lenel Certified Technician. Any access to the System Architecture or Data Communication infrastructure of NAUPASS requires that vendor apply for and secure Affiliate Status with the University. The assigned Project Manager shall at a minimum be an affiliate for this purpose along with the installer if appropriate based on size and scope. For additional information regarding affiliate status, visit:

<http://www4.nau.edu/louie/affiliation.html>.

PROJECT MANAGEMENT

Integrator shall provide a Project Manager who is experienced in the administration and supervision of the security field and electrical work, both within the various types of security integration and with relation to other types of work and who is hereby authorized to act on behalf of Integrator. The project manager responsibilities will include but are not limited to providing schedules, attending project meetings, submittals, safety, quality control, and testing, training and as-built documentation. The project manager must be an employee of Integrator and working in the security field

Section Title
Number

28 23 13 Video Surveillance Control and Management System

Digital Video Recorders (DVR) must be compatible with established NAUPASS (Lenel) infrastructure, and allow live and recorded video to be viewed through the version of Lenel OnGuard Alarm monitoring software in use by Northern Arizona University at the time of installation.

Initial configuration of DVR should conform to the following minimum quality settings.

Minimum Initial Configuration Settings

Recording mode	Frames per second	Resolution
Live	2 fps	640 X 480
Normal	2 fps	640 X 480
Event	3.75 fps	640 X 480

28 23 19 Digital Video Recording Devices

The following equipment is a list of video surveillance digital video recording equipment that is approved for installation on campus:

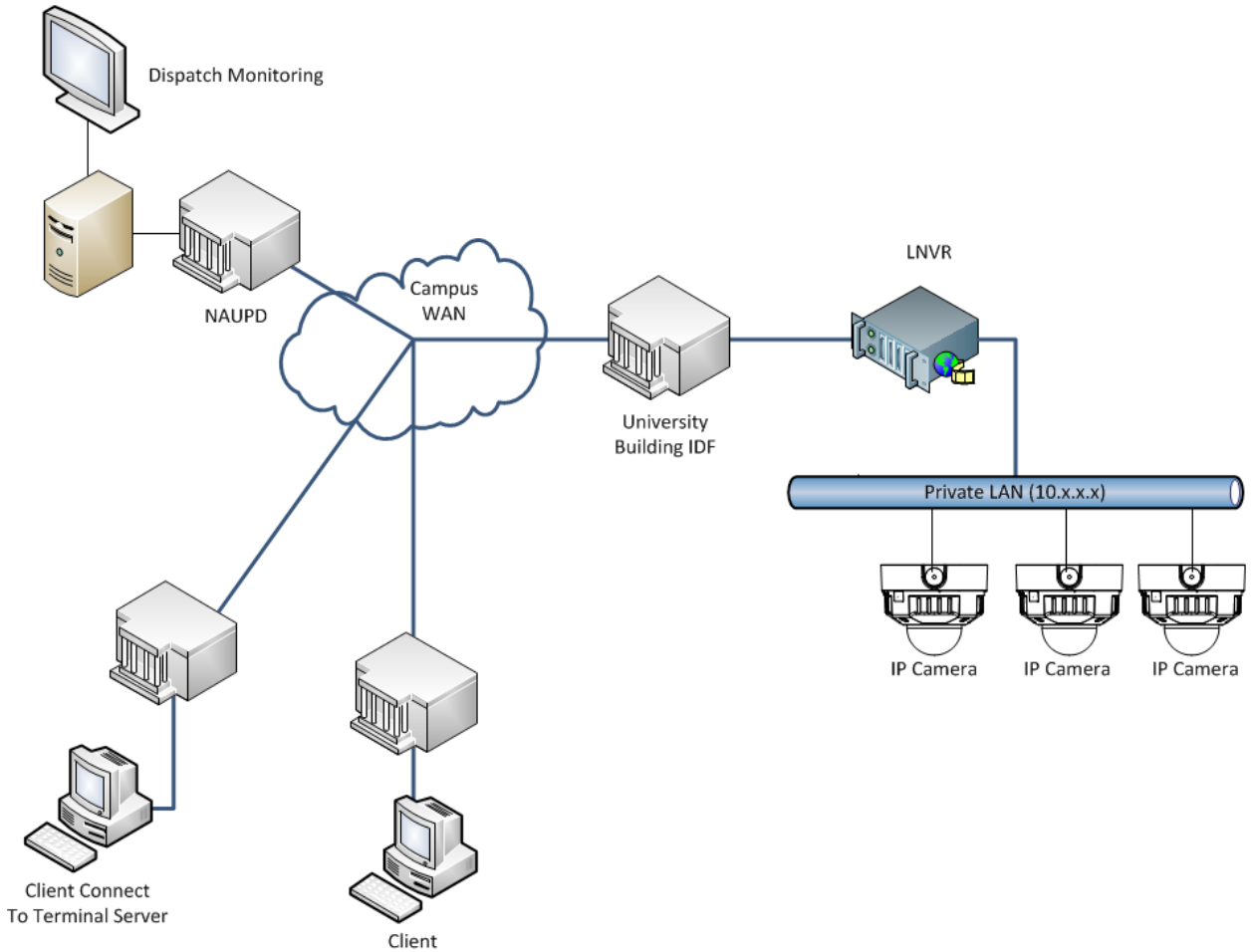
- Lenel NVR7 models: DVC-LP, DVC-LP2, DVC-ST, DVC-SE, DVC-EX, DVC-HD
- Comparable physical or virtual systems which meet following minimum criteria and are approved by NAU CSA-IT

Minimum System Requirements

Chassis	1, 2 or 3 RU rack mountable
Processor	Dual Core 2.0 GHZ processor or better
RAM	4 GB
Operating System	Desktop:Windows 7 SP1 Pro or better. Server: Microsoft Server 2008 R2/SP2 or better *32 bit or 64 bit is acceptable.
Hard Drive capacity	**** Varies depending on number of attached cameras. 500GB
Hard Drive Configuration	1 dedicated system drive. 1 dedicated data (video storage) drive
On board Cache	16MB
Software Version	Lenel Video Suite 7.0.825 or better

- No more than 36 video surveillance remote devices per DVR without exception from CSA-IT
- NVR’s must have uninterruptable power supply capable of providing a minimum of 60 minutes of continuous power in the event of power disruption.

Section Number **28 23 23** Title **Video Surveillance System Infrastructure**



28 23 29 Video Surveillance System Remote Devices and Sensors

DESCRIPTION

All video surveillance remote devices must be listed as compatible with Lenel OnGuard Software and integrated with established campus infrastructure systems. All video surveillance remote devices including cameras, motion and intrusion detection devices used to trigger video surveillance, alarms, and recording equipment must be able to be managed by the OnGuard system.

In addition, all video surveillance cameras shall:

- Be on the current schedule of acceptable Cameras maintained by Campus Services and Activities IT
- Be digital, transmitting data utilizing Internet Protocol (IP).
- Support a minimum resolution of 720X1280.
- Have the ability to be powered by Power over Internet (PoE).
- Support motion detection
- Be Open Network Video Interface Forum (ONVIF) Compliant.

Section Title
Number

ACCEPTABLE CAMERAS

The following models have been approved for use on campus. Substitutions may be made with approval from CSA-IT.

Indoor cameras:

1. Axis Q7406
2. Panasonic WV-NF302
3. Panasonic WV-SP306
4. Sony SNC–DH140
5. Sony SNC-DH180

Outdoor Cameras:

1. Axis Q1755
2. Sony SNC-DM160

28 26 00 Electronic Personal Protection System

DESCRIPTION

The operation and maintenance of any Electronic Personal Protection Systems falls under the authority of NAUPD and the individual university department or administrator as designated by the appropriate Vice President. Any and all additions, changes, or modifications shall be coordinated with NAUPD and the department administration prior to commencement of activity.

28 30 00 ELECTRONIC DETECTION AND ALARM

28 31 00 Fire Detection and Alarm

Approved fire alarm equipment manufactures and control panels:

Notifier:

NFS2 - 3030

NFS2 - 640

NFS – 320

General

Installation contractor shall be a factory certified authorized distributor – Notifier.

System designer – Fire alarm system plans and specifications shall be developed in accordance with NFPA 72 by persons who are experienced in the proper design, application, installation, and testing of fire alarm systems. System installer – installation personnel shall be supervised (to include conduit, boxes and wiring installation) by persons who are qualified and experienced in the installation, inspection and testing of fire alarm systems.

Section
Number Title

Qualified personnel shall include, but not limited to, the following:

- *Personnel who are factory trained and certified for the alarm system installation of the specific type and brand being installed.*
- *Personnel who are certified by a nationally recognized fire alarm certification organization.*
- *Personnel, who are registered, licensed or certified by a State or local authority.*

System Requirements

All new Fire systems shall be addressable. All fire alarm equipment, components and software shall be nonproprietary and shall be completely field programmable by Northern Arizona University Fire/Life Safety Personnel (NAU-FLS).

All new fire alarm systems shall provide In-Building Fire Emergency Voice/Alarm Communication System (EVACS) with female voice. The evacuation messages shall be preceded and followed a minimum of two cycles of the emergency evacuation signal – Three-pulse temporal pattern.

The following requirements shall be met for lay-out and design:

- *The speaker layout of the system shall be designed to ensure intelligibility and audibility.*
- *Intelligibility shall first be determined by ensuring that all areas in the building have the required level of audibility.*
- *The design shall incorporate speaker placement to provide intelligibility.*
- *System design shall incorporate designation of acoustical distinguishable spaces (ADS).*

Contractor shall provide all access-login codes, programming software and minimum four (4) hours training to include all aspects of panel functions, operation, programming and trouble/repair procedures.

Fire Alarm Control Panel (FACP) shall provide communication capabilities:

- *Notifier NFN Gateway and all required equipment.*

All Academic building Fire Alarm Systems shall include at a minimum detection in all the following areas; all corridors, hallways, mechanical, electrical, telecom equipment rooms. Additional detection may be required in other hazardous locations as identified during the NAU Fire Marshal review. All residential buildings shall be “total detection” systems and shall provide addressable detectors with sounder bases and visual appliances in all suites/sleeping areas. Addressable in room detector shall report as a supervisory at the main panel.

Section Title
Number

All addressable devices and equipment shall provide an external label indicating SLC loop and address.

All academic buildings shall be provided with manual pull stations installed in accordance with NFPA 72.

All residential buildings shall be provided with at least one (1) common area manual pull station.

All building manual pull stations shall be provided from all independent exits from mechanical, electrical and other service or remote exits.

The designated primary entrance shall provide FACP or a remote fire alarm annunciator with required communication equipment.

Main FACP/Remote annunciator displays shall be mounted at a height of 64 inches from the floor to the centerline of the display.

All auxiliary panels (NAC Power) shall be mounted at a height of 64 inches from the floor to the top of the enclosure.

Pull stations shall be mounted at a height of 48 inches from the floor to the centerline of the pull.

All wall mounted visual /audio devices shall be mounted at a height of 80 inches from the floor or 6 inches below the ceiling to the centerline of the device whichever is lowest.

External battery boxes shall be specifically designed and approved for the purpose of housing batteries and shall be mounted immediately below the main FACP. Battery boxes shall not be installed in sub floors.

Fire alarm detection devices shall be installed as per their listing. Spot type smoke detectors shall be spaced at the detectors UL listing – open areas, corridor, hallways not to exceed 30 feet unless approved by NAU-FLS prior to installation.

All beam and duct detectors shall provide remote test/ indication devices.

There shall be no carry-over pre-existing sub-panels in the final system.

All exposed surface mounted fire alarm pull stations, audio-visual devices shall be mounted on back boxes specifically designed for the purpose or provide approved skirts – no exposed boxes with knock-outs (except in areas not normally occupied by the general

Section Title
Number

public – mechanical, electrical rooms, etc.).

Fire Alarm circuits shall be identified at the terminal and junction locations. Identification “Key” or “Legend” shall be consistent with approved installation and as-builts drawings.

All wiring shall be installed in metal raceway – ½” or larger. Flexible Steel Conduits (Maximum 6 foot whip) shall be used only where approved by NAUFM for connection to equipment which is moveable; connections from a close by junction box to lay-in type device in a “T” grid ceiling. The maximum fill ratio of raceway shall be 50% of the NEC maximum fill. Any exceptions to this requirement shall be specifically granted by NAUFM.

All fire alarm system conduit, junction boxes, and covers shall be painted red and “J” box covers shall be labeled in bold 1” black decal letters “F/A.”

Existing system shut-down shall be coordinated with Fire Life Safety @ 928-523-4227

Inspections and Final Acceptance

All conduits, boxes, fittings and equipment back boxes shall be inspected by NAU Fire Life Safety. No work can be covered up prior to installation inspection. Inspection request shall be in accordance with Division 1.

At system acceptance the Contractor shall provide:

- *All relevant manual(s), Technical/Maintenance manual(s),*
- *Complete As-builts indicating and accurate map detailing:*
 - *All system circuits routes and individual circuit identification,*
 - *Device and equipment locations*
 - *Device address*
 - *EOL locations.*
 - *Auxiliary equipment locations*
- *NFPA 72 Certificate of completion*
- *100% System test printout.*
- *Two (2) copies of the complete system programming disc.*

No approval (Green tag) will be issued unless all required information and documentation is provided at the time of final acceptance.

Contractor shall provide three (2) year complete warranty on all system components, programming and installation.

Contractor shall have an in-place support facility with technical staff, spare parts inventory, and all necessary test and diagnostic equipment. Contractor shall provide 2

Section Title
Number
hour emergency response time.