Technology Infrastructure Master Plan
Volume 4 – District Standards
Section 5

and

Electronic Security System Standards
Volume 4 – District Standards
Section 6

Board of Trustees Meeting
Tuesday, October 9, 2007
MARIN COMMUNITY COLLEGES

ELECTRONIC SECURITY SYSTEM STANDARDS

Tomasi-Dubois & Associates
August 29, 2007
<table>
<thead>
<tr>
<th>Part</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General Requirements</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Performance Standards</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Design Standards</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>Product Standards</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>Installation Standards</td>
<td>66</td>
</tr>
</tbody>
</table>
PART 1  GENERAL REQUIREMENTS

1.01  PURPOSE

A. The following was developed to address the security needs of the Marin Community Colleges (College):

1. The security systems will be designed to reduce criminal opportunity by providing real-time alarm and video surveillance while restricting and controlling access to certain levels and areas of Marin Community College facilities, and by enhancing the ability to detect, evaluate, and respond to, or cause a response to, criminal activity.

2. This will be accomplished by developing an Integrated Electronic Security System (IESS).

B. The IESS is intended to achieve the following objectives:

1. Provide campus-wide systems management through centralized policy development and execution.
2. Control access to selected areas with a proximity-card access control system. (Presenting an authorized card to a surface-mounted card reader will allow access through the controlled door.)
3. Communicate security signals from areas provided with, or other entry ports equipped with, intrusion detectors, panic switches, and tamper devices to indicate:
   a. Detectors operative, no alarm
   b. Detectors operative and in alarm
   c. Detectors rendered inoperative
4. The IESS will be modular and designed to permit expansion by the addition of more or new detection, CCTV, and/or access control devices. This will be accomplished without requiring significant change in the construction or configuration of Security Operations Center (SOC) or Contract Police Dispatch Operations Center (DOC) equipment.

1.02  OVERVIEW

A. The IESS will consist of a policy based converged security management system.

B. The following integrated systems specified, installed, and operating in such a manner so as to reliably assure the continuous reception at and transmission from the sites and SOC’s of all alarm and other communications inputs and all automatic outputs:

1. SECURITY SYSTEM MANAGEMENT SOFTWARE, comprised of a Security Management System software package, reliably operating on a current Windows based platform, with the capability of managing both alarm and video resources.
2. ACCESS CONTROL SYSTEM, comprised of access-control and photo-badging workstations, proximity card readers, door control panels, electric-locking hardware, hands free (request for exit) PIR detectors, magnetic door contacts, and power supplies, as well as required wire, cable, fittings, adapters, key-operated enclosures and necessary components to perform the specified functions.

3. INTRUSION DETECTION SYSTEM, comprised of magnetic door contacts, local sounders (if requested), panic buttons (switches), tamper switches, and all related wire, cable, fittings, and adapters necessary to power and communicate activation to the Access Control Subsystem.

4. VIDEO SURVEILLANCE SYSTEM comprised of cameras, power supplies, digital video recorders, video workstations and all related cabling, wiring, fittings, and adapters necessary for real-time communications between the sites and the SOC.

5. COURTESY CALL STATIONS comprised of wall mounted or free-standing units with a combination always on blue-light location marker and hi-intensity blue strobe that comes on when the call button is pressed. Two-way communications is established when the call button is pressed and the unit dials a pre-programmed phone number and makes connection.

C. The IESS will be monitored at the SOC and DOC with the via the access control server and workstations at the Kentfield Campus and a work station at the DOC.

1. Campus facilities will have controller panel(s), card readers, and alarms communicating via Local or Wide Area Networks (LAN, WAN) to the SOC Global Server.

2. If there is a communications loss between the controller panel and the Global Server, the Controller Panel will store the transactions and alarm events until communications is re-established.

3. If it is critical to have rapid local response to alarm events then a Central Station Communicator (Auto Dialer) will also be installed and connected to a central station alarm monitoring company where available.

D. Video monitoring will be provided at designated locations as indicated below, and recorded at each facility using a Digital Video Recorder.

1. The video recording device will be connected to the WAN so that video from these sites may be viewed “Live” or replayed from the SOC and DOC or any other authorized locations.

E. Overall data transmission will be via wired and wireless network.

1.03 DOCUMENTATION AND DRAWINGS

A. Preliminary Submittals:

1. Prior to purchasing any equipment, the Contractor will submit, for acceptance the following:
   a. A material list with names of manufacturers, model numbers, and technical information on all equipment proposed for installation
b. Catalog cut sheets of the equipment to be installed

c. A preliminary schedule based on installation events

B. Project Record Drawings:

1. The purpose of Project Record Drawings is to provide factual information regarding all aspects of the project and to enable and support future service, modifications, and additions to the Security System.

2. The Project Record Drawings are an important element of this project. The Contractor will accurately maintain the Project Record Drawings throughout the course of this project.

3. One (1) set of Security Drawings on electronic media and/or reproducible media may be requested in writing from the College for Contractor use in developing submittals and Project Record Drawings.

4. An individual skilled in standard drawing practices will produce the final set of Project Record Drawings.

5. One (1) week before the scheduled test and final acceptance of the work, the Contractor will deliver one (1) complete set of Project Record Drawings (on Bond) and AutoCAD® drawing files in “DWG” or in “DXF” format on a CD-RW.

6. The Project Record Drawings will, at a minimum, include the following:
   a. Floor plan drawings indicating wire routing (wire routing will be delineated in straight-line runs and be tagged with cable identification and terminal strip numbers to coincide with the installation)
   b. Floor plan drawings indicating device locations to include any existing equipment, wiring, conduits, and raceways that were reused in this project with device legends
   c. Functional one-line diagrams for each subsystem
   d. Wiring details showing rack elevations, equipment wiring and terminations, and inter-rack wiring
   e. Wiring diagrams for all custom circuitry including interfaces to various output controlled devices (i.e., overhead doors, sliding doors, parking gate operators, fire alarm system interface, etc.)
   f. Typical point-to-point wiring diagrams with wire color for each piece/group of equipment within the system
   g. Layout details for each riser location - including security panels, PSs, J-Boxes, conduit, and any other security-related equipment located in the riser

C. System Documentation:

1. The System Documentation will be compiled into a binder, or set of binders, with easy identification as to its contents. Each binder will be organized into tabbed sections. There will be a master index identifying the contents of each binder and section.

2. The Contractor will also deliver (along with the Project Record Drawings) the System Documentation Manuals to the College, including the individual factory-issued manuals containing all technical information on each piece of equipment installed.

3. The System Documentation Manuals will include, at a minimum:
a. An operational description of each subsystem
b. Detailed programming descriptions for each subsystem, including step-by-step procedures, with illustrations identifying how computer screens will look after each entry
c. Explanations of subsystem interrelationships, including operations of each subsystem, operations unique to the interfaces between each of the subsystems, and possible conflicts that may occur with the interface (each explanation will be identified, tagged, bound, and indexed into a single binder)
d. Electrical schematics for each piece of equipment furnished
e. Power-up and power-down procedures for each subsystem
f. A description of all diagnostic procedures
g. A menu tree for each subsystem providing a graphical flow of commands within the menu system
h. Setup procedures for each component of the subsystems
i. A list of manufacturers, their local representatives, and subcontractors that have performed work on the project (include contact names, phone numbers, and addresses for each)
j. Installation and service manuals for each piece of equipment
k. Maintenance schedules for all installed components, including inspections and preventative maintenance schedules, and documentation of all repaired or replaced equipment
l. Descriptions of all software, their terms and functions, as well as required sequences
m. A directory of all disk files
n. A description of all communications protocols including data formats, command characters, and a sample of each type of data transfer
o. Instructions for manufacturer-supplied report generation, with illustrations showing how reports should look, and screen-by-screen illustrations for each entry made
p. Instructions for custom report generation
q. Database format and data entry requirements
PART 2 PERFORMANCE STANDARDS

2.01 GOVERNING CODES AND RELATED STANDARDS

A. Except as modified by governing codes, the Contractor will adhere to all applicable provisions and recommendations of building, regulatory, equipment manufacturer and the College standards applicable to the project.

B. All work will conform to the most current version of the following codes and standards, where applicable; and when a conflict occurs Contractor will follow the most stringent requirements:

1. California and Federal OSHA requirements.
4. National Electrical Code, in particular NEC Sections 600-3(b) and 800-3(d), and applicable local electrical code.
6. Underwriters' Laboratories (UL).
7. FCC CFR 47 part 68 subpart F
8. IEC 60603-7
10. Institute of Electrical and Electronic Engineers (IEEE).
13. ANSI / EIA / TIA-568, Commercial Building Telecommunications Wiring Standard
14. ANSI / EIA / TIA-569, Commercial Building Standard for Telecommunications Pathways and Space
15. ANSI / EIA / TIA-606, Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
16. ANSI / EIA / TIA-607, Commercial Building Grounding/Bonding Requirements
17. ANSI / EIA / PN-3398, Additional Horizontal Cabling Practices for Open Offices
18. ANSI / EIA / PN-2498, Technical Specifications for 100 Ohm Screened Twisted Pair Cabling
19. ANSI / NFPA 70, National Electric Code
20. BICSI, Telecommunications Distribution Methods Manual
21. EIA / TIA 568, 569, 606, 607, All current and past Technical Service Bulletins

2.02 CONTRACTOR QUALIFICATIONS AND REQUIREMENTS

A. Maintain the appropriate Contractor’s and other licenses required to perform the type of work stipulated by the specification.

B. Be a certified dealer of the specified equipment, with proven experience in comparable installations of this size, type, and scope within the last five (5)
years. (A list of installations, including contact name and phone numbers, will be submitted to the College upon request.)

C. Employ factory-trained personnel in the installation, operation, and maintenance of the subsystems. At least one (1) member of the installation team will have a minimum of two (2) years experience in the installation, operation, and maintenance of the access control system to be provided.

D. Provide qualified electronic technicians (as described above) to hook up, program, and test final termination (journeyman electrical workers may be used to install conduit, raceways, and wiring). All such work will be supervised by the Contractor’s Project Manager.

E. Provide twenty-four- (24-) hour support services from an existing operations center within eighty (80) driving miles of the College’s Facility.

F. Provide emergency service within four (4) hours of notification.

G. Provide factory-trained service personnel who are dedicated to the College’s account. Any changes in personnel will be approved by the College prior to any new service technician’s work on the account. (All costs for assigned service technicians will be included in the contract price.)

H. Have the capability to perform system testing and provide instruction on the use and operation of all elements of the subsystems and their interconnections.

I. Provide qualified instructors to conduct factory system training.

J. Maintain an inventory of spare parts and other items critical to the system operation (and as necessary to meet emergency service requirements of this project) within the local service center to allow for minimal downtime of critical elements of the College’s Security System.

K. Provide local in-house engineering and project management capabilities consistent with the requirements of this project.

L. Provide a full-time project manager who will be present while the work is actively in progress, and who will be the same individual throughout the course of the project. This Project Manager will be responsible for system programming, preparation of Operation and Maintenance Manuals, training programs and schedules, test protocols, documentation of system testing, maintenance of Record Drawings, and coordination and scheduling of all subcontract labor. (the College reserves the right to approve the Contractor’s project manager.)

M. In the event the Contractor becomes unable to complete the work in accordance with the contract documents or to the satisfaction of the College due to a lack of understanding of equipment, systems or services required by the contract documents, it will be the responsibility of the Contractor to retain the services of the applicable manufacturers’ representatives or other qualified contractor to expeditiously complete the work in accordance with the construction schedule (with no additional cost to the College).
2.03 INSPECTIONS

A. The College will visit and inspect work progress and status during course of project.

2.04 TESTING AND CERTIFICATION

A. The Access Control, Alarm Monitoring, CCTV, and Video Badging System will be tested in accordance with the following:

1. The Contractor will conduct a complete inspection and test with the College of all installed access control and security monitoring equipment.
2. The Contractor will provide staff to test all devices and all operational features of the system for witness by the College and the Authority having jurisdiction.
3. The College prior to acceptance must witness all testing.
4. The testing and certification will take place as follows:
   a. All deficiencies noted in the above test will be corrected.
   b. Test results will be submitted to the consultant or College’s representative.
   c. System test witnessed by College’s representative and correction of any deficiencies noted.
   d. The College’s representative will accept the system.

B. In the event of discrepancies or deficiencies, Contractor will make good on repairs within ten (10) days of notification by College.

C. Final acceptance will occur when all discrepancies and deficiencies are reconciled and all documentation has been received by the College.

2.05 SYSTEM TRAINING

A. Qualified personnel will be provided to train key College-selected personnel in the operation of the installed Security System.

B. The training program will be designed to provide a comprehensive understanding and basic level of competence with the system.

1. It will be sufficiently detailed to allow the College’s personnel to operate the system independent of any outside assistance.
2. A comprehensive lesson plan covering all Security System component operations, configurations, and maintenance will be submitted as part of the submittal process.

C. Training session will be limited to a maximum of four (4) hours per day, unless longer sessions have been agreed upon.

D. At least one (1) refresher training session will be provided after the system has been operational for three (3) months.

E. All training will be completed onsite using the College’s equipment unless off-site
training is agreed to be more advantageous to the College.

1. If off-site training is agreed upon, the cost for such training will not be any greater than if the training was conducted on-site.

2. If training is off-site, it will be done on a complete and operational system that is parallel and equal to the system being installed for this project.

2.06 WARRANTY

A. As per the guidelines set forth by the State Contractors Association, Contractor will provide a one-year written warranty covering material and workmanship.

B. Contractor will comply with any additional warranty requirements contained within written specifications provided by the College.

C. All repairs related to workmanship and material deficiencies will be made at no cost to College during the warranty period.

D. Contractor will provide to the College warranty information covering parts & materials used by Contractor.

E. Warranties will include a ninety day stability period to insure reliable system operation.
PART 3 DESIGN STANDARDS

3.01 GENERAL

A. The security system will be designed and developed according to the following guidelines and configurations.

3.02 SECURITY OPERATIONS CENTER (SOC/DOC)

A. The SOC located in the Police Department facilities of the Kentfield campus will be capable of monitoring all campus facilities, via the system server and workstations. The workstation located in the DOC will be capable of providing the same monitoring.

B. The SOC will be manned eight hours per day, five days a week. The DOC will serve as the primary monitoring point for the remaining times to for allow 24/7 monitoring.

C. Personnel working in the SOC and DOC will have up-to-date contact information for all facilities as well as instructions on when they should intervene regarding alarm activity or any other suspicious activity at any site.

D. All functions of the IESS (e.g., monitoring of alarm and supervisory events, database management, modification of cardholder database, logging of authorized as well as unauthorized events, etc.) will be managed and controlled by the SOC Command and Control Subsystem servers.

E. The SOC will be equipped as follows:

1. Multiple 24-inch or greater Liquid Crystal Display (LCD-TFT) with:
   a. Software that will display overall campus maps with system control icons overlaid
   b. Integrated video on additional displays
2. An Access Control Server
3. Security Management Server software
4. Video Management Software
5. A separate video reviewing workstation with 20 inch LCD monitor (may be located in a separate office)
6. Digital Video Recorders
7. A video switcher and CCTV display controller (optional if needed for faster PTZ control)
8. Administrative workstation(s) for reports, emails, and general administrative work
9. A console (desk) sufficient for at least two (2) operators
10. Miscellaneous supplies

F. The DOC will be equipped as follows:
1. Two (2) 22-inch LCD-TFT displays for access control and video monitoring
2. An Access Control Work Station
3. Software
   a. Access Control Application
   b. Video Application
   c. Operating and College required applications (i.e. anti-virus software)
4. Miscellaneous supplies

G. Photo-Badging:
   1. At the Kentfield Campus Police facility, a small room or office will be designated for photo-badging.
   2. A photo-badging workstation, camera, lighting and, badge materials will be kept in the room.
   3. The workstation will be connected to the Access Control Server.
   4. Employees and contractors will report to the room to obtain a badge (credential) for access through card-reader-controlled doors.

H. Human Resources (HR) Interface:
   1. The Access Control Server will have software installed to interface with the HR Personnel Management software.
   2. Data communications will take place between the HR system and the security system, and will be implemented campus-wide.
   3. When a new employee’s data is entered into the HR system, the data required by the security system will be sent to the Global Access Control Server to facilitate the badging process.
   4. Upon termination, the person’s card will be immediately deactivated from the security or HR systems, disallowing entry into any Marin Community College College facility.

3.03 ACCESS CONTROL/INTRUSION DETECTION FACILITY (SITE) CONFIGURATION

A. Access cards distributed from the Campus Police Department.
   1. All employees will be issued the same proximity card.

B. Each facility will have one (1) or more card readers controlling doors, and:
   1. The card readers will be controlled by an access control panel (door controller) capable of controlling multiple doors.
   2. A Typical door will have the following devices:
      a. An HID-compatible proximity card reader
      b. A magnetic reed door alarm contact for each leaf of a doorway
      c. A hands-free request-to-exit device to momentarily disable the alarm contacts when exiting through a controlled door (typically a passive infrared detector [PIR])
      d. Electrically-operated door hardware
      e. Any additional devices (door-override switch may be required
3. Doors controlled by card reader:
   a. Main lobby doors
   b. Other exterior doors deemed advantageous for employee entry
   c. Doors coming from the lobby into a facility space
   d. Server room doors
   e. IDF room doors
   f. Other doors requested by the user and approved by security

C. Doors on the perimeter not controlled by card access will have, as a minimum, a magnetic reed door alarm contact for each leaf of a doorway.

D. Any additional openings, such as operable windows on the perimeter of the facility, will have detection devices.

E. One (1) or more access control workstations will be provided at designated facilities located at an HR desk, with the following:
   1. The workstation will be capable of monitoring card and alarm activity for the campuses.
   2. The security system access control server will gather all card transaction and alarm data from the access control panels at each site via the Marin Community College College’s WAN.
   3. All data collected within the region by the access control server will be available at each site’s workstation via the WAN.
   4. Each workstation will be set up to perform system configurations associated with the campuses and be password controlled.

3.04 VIDEO SURVEILLANCE FACILITY (SITE) CONFIGURATION

A. The video surveillance system will be comprised of IP addressable cameras to provide a visual record of events surrounding designated areas.

B. Cameras will be used to monitor the following areas:
   1. Card-controlled perimeter doors.
   2. Campus server rooms
   3. MDF/IDF rooms where designated
   4. Money handling areas and be connected to a panic alarm located at the desk.
   5. Other areas as requested by the College.

C. Video will be displayed on designated monitors/workstations in the SOC and DOC.

D. Video associated with locations that have alarm inputs will be programmed to be displayed on a monitor upon alarm activation.

E. The system will be capable of “pop-up” video on the access control system displays and instant replay of pre-alarm video by clicking on access control alarm
icons.

F. Each campus will have one or more video recorders with mass storage to archive up to thirty (30) days of recorded video.

G. Video will be recorded continuously at a rate of at least 1 frame per minute in a low resolution mode with recording rate and quality increased when an alarm is activated or motion is detection in sensitive areas.

H. The system will have the capability to send video information to police Computer Aided Dispatch (CAD) system in the patrol cars via wireless network.

3.05 COURTESY CALL STATION (SITE) CONFIGURATION

A. A ring-down phone with preprogrammed phone numbers that are called when call button is pressed and an associated steady-on and blue strobe will comprise the Courtesy Call Station.

B. Courtesy call stations will typically be placed in parking areas and other designated locations on each of the campuses based on College staff input.

C. The call stations will typically be a nine (9) foot pole with call station electronics incorporated in the pole and a blue light on top.

D. The pole will have the word “COURTESY CALL” displayed in large letters on the pole.

E. A steady blue light will provide a beacon for potential users in locating the call station and the blue light will change into a high intensity strobe when call button is pressed.

F. Cameras will be located near the call stations for rapid identification of activity at and around the call station.

G. Call station will be integrated with the security management software so that when a call button is pressed the location of the call station will be displayed the system map display.
PART 4  PRODUCT STANDARDS

4.01  GENERAL

A. The contractor will be responsible for installing all products in accordance with the manufacturers' and accepted industry materials and installation standards.

B. All products will be new and current in production at the time of installation and available from manufacturers with multiple installing vendors near (within eighty [80] miles) the Colleges.

4.02  SECURITY MANAGEMENT SOFTWARE

A. The System platform will offer a complete access control solution; alarm monitoring, video imaging, badging and CCTV control.

B. Terminal Services
   1. The System will support Windows 2000 Terminal Services.
   2. Terminal Services will allow the System server application to reside on the Windows Terminal Server while client access will be obtained via a standard web browser interface.
   3. Operating systems supporting a standard web browser will be capable of utilizing the thin client architecture.
   4. The System will support unlimited connections, based on concurrent licensing, to the System software.
   5. Full functionality will be obtained through the intranet connection allowing full administration and monitoring without the need for a local installation.
   6. This functionality also allows video badging and image capture to occur remotely without the need to install the application locally.

C. Operating System
   1. The System will support Windows 2003 Server as the host Operating System.
   2. It will support XP Professional as a client Operating System.

D. Relational Database Management System
   1. The System will utilize the Microsoft SQL Server relational database management system.

E. LDAP/ Microsoft Active Directory Services
   1. The System will provide support of LDAP (Lightweight Directory Access Protocol) for enabling the user to locate organizations, individuals, and other resources such as files and devices in a network.
   2. The System will provide a direct link to Microsoft Active Directory
Services.
a. This integration will allow for a centralized data repository that can be utilized by systems throughout a network.
b. The System will allow the transfer of Active Directory users via the Data Transfer Utility.
c. Active Directory users may be imported into the System database. Conversely, System users will be capable of being exported to the Active Directory.

F. OLE-DB
1. The System will utilize Microsoft’s OLE-DB object-oriented, database access method.
a. Microsoft’s OLE-DB method will provide support of not only relational databases, but also to “hierarchical data sets” such as Microsoft Exchange stores and XML record sets.
b. OLE-DB will allow easier integration of disparate data sources.

G. Encryption
1. The System will provide true 128-bit data encryption between the host and door controllers.

H. Password
1. The System will use an integrated authentication method, which utilizes Windows user accounts and policies.
2. Client stations will function under the Microsoft recommended default user rights.
3. Passwords must support scheduled expiration and be capable of prompting the user for a password change automatically as a part of the Windows login process.
4. Additionally passwords will support complexity rules such as length of password and required number of alphanumeric characters as established by the Windows policies regarding user accounts.

I. Information Access
1. The System will be capable of limiting operator access to sensitive information.
2. Operators will have proper authorization to edit the information.

J. Shadow Login
1. The System will allow users to login over a currently logged-on user without having the current user log off the System or Windows 2000.
a. For example, the System will allow an administrator to login over a restricted class user to perform a function on the System that the current user doesn’t have permission to perform.
b. This provides a level of security in that the user’s workstation will never need to go offline or be unattended.
K. User Friendly Graphical User Interface

1. The System will be fully compliant with the Microsoft graphical user interface (GUI) standards, with the look and feel of the software being that of a standard Windows application, including hardware tree based system configuration.

2. The System will provide user definable “drag and drop” Hardware Templates in order to simplify the system setup and maintenance.
   a. The user interface will be designed such that the ability to add resources such as time zones, clearance codes, alarm types, etc. will be available within the functions which they are used rather than requiring the user to close the function and navigate to another section of the application to add the resource.

3. The System will provide a dependency search to allow the user to determine all the dependencies of hardware devices in the configuration trees.
   a. The search function will display the list of assignments at the logical device level to assist the user to select all appropriate devices when removing an object from the configuration.

4. The system will support of graphical user manager utilities (Wizards) to ease the enrolment process for Users, Controllers, Communication Channels, Badge holders, and Logical Devices.
   a. The wizards will be made available through a Welcome screen at main application entry as well as at the individual resource creation point.

L. Help

1. The main System user interface will include a help icon, which will require only one click to activate.

2. The standard special function key “F1” will have the capability to be programmed to provide access to the help system.

M. Guard Tour

1. The System will include a guard tour module, which will allow the user to program guard tours for their facility.
   a. The tours will not require the need for independent or dedicated readers.

2. The System will provide the ability to use the same logical device more than once in a guard tour.
   a. The Logical device will be selected from a resource box located on the left side of the screen.
   b. Selecting this box will bring all system readers to view for tour selection.

3. Once a Logical Device has been selected a dialogue requesting the ‘Time’ required reaching designation will appear.
   a. This entry will be in military format (00:00) and represents the amount of time required to reach each checkpoint.

4. After the ‘Time’ has been entered, the tolerance needs to be entered, the ‘+’ and ‘-’ values will be defined.
a. A text box will allow the user to enter the time tolerated for early and late arrivals.

5. The user will be able to ‘Start Guard Tour’ in the Guard Tour screen, and bring up a ‘Select Guard’ dialogue box.
   a. Selecting a Guard from this list will assign that user (guard) to that tour.
   b. The listing of guards that appear in the dialogue box will be pulled from the cardholder screen.
   c. The cardholder screen includes a ‘Guard’ checkbox.
   d. Selecting this box will register the badge holder/cardholder as a ‘Guard’ with the capability to run tours.

6. If the times defined in the tour are not met within the time allotted, an alarm will be sent to the monitor.

7. The user will have the capability to run multiple tours simultaneously.

N. Status Groups

1. The System will support a real-time system status monitor that graphically depicts all logical devices.

2. The Status Groups window will be a split window with Logical Device icons displayed in the upper portion and the Device Types associated with a selected Logical Device displayed in the lower portion.

3. The Status Groups will be available in the Hardware Configuration view and the alarm monitor view.

4. Upper view
   a. The icons representing each logical device within this view will change based upon the status of that logical device.
   b. Different icons will be available to indicate:
      1) Normal State
      2) Indeterminate State
      3) Reader Off-Normal State
      4) Input Off-Normal State
      5) Output Off-Normal State
      6) Reader and Input Off-Normal State
      7) Reader and Output Off-Normal State
      8) Input and Output Off-Normal State
      9) Total Alarm State

5. Lower view
   a. Individual Devices Types (readers, inputs, outputs which are further defined as door position switches, request-to-exit devices, enunciators, etc.), which make up the selected logical device, will be displayed in the lower view.
   b. This lower view will include an icon for each device type and indicate the category (input point, output point, reader) and the status of the individual device types that make up the logical device (normal, energized, locked, unlocked, in-alarm) Note that when a reader device type is not in an off-normal status, the reader mode is displayed (card-only, PIN-only, Card and PIN, Card or PIN)

6. Status Group Filter
   a. The Status Groups window will be filterable to show only Logical
Devices, which are currently in an off-normal condition based on the following:

1) Reader Filters
   a) Unknown
   b) Disabled
   c) Locked Unlocked
   d) Facility Code
   e) Timed Override

2) Input Filters
   a) Alarm
   b) Trouble
   c) Held Open
   d) Forced Open
   e) Open Circuit
   f) Short Circuit
   g) Exit Warning
   h) Hardware Masked
   i) Software Masked
   j) Offline

3) Output Filters
   a) Energized
   b) Trouble
   c) Hardware Masked
   d) Software Masked
   e) Offline

O. Keyboard Accelerators

1. The System will allow the user to use a shortcut key to enable designated system commands.
2. The System operator will have the capability to set up accelerators for two options, Commands and Event Procedures.
3. The operator will have the capability to add, edit, and delete accelerators for commands and event procedures, as well as grant or revoke user access to these options.
4. The keyboard accelerator dialog box will include a user definable description, the New Shortcut Key Combination (For example Ctrl+Shift+T), Check boxes for Command Procedure and Event Procedure with drop down lists.
5. The Keyboard Accelerator icon will be displayed in the right System pane, for single mouse click execution.

P. Void Card Upon Lack of Use

1. The System will allow system operators to set a pre-defined time period in which cardholders must swipe their card through a card reader in the System.
2. The System will automatically void the card if the defined timeframe has elapsed without a card read since the card was created.

Q. User Functions and ADA Ability
1. The System will provide User Functions and ADA ability that provides the capability to trigger an event at the System Intelligent Controller when a defined card is presented.
2. The Extended Strike Time and Extended Held Time for a reader will be utilized when a card with ADA checked is presented.
3. Triggers set off by a card read will include a given user level.
   a. This functionality will allow only certain users, based on their access privileges, to trigger events at the door.

R. Pathways
1. The System will support the capability of programming Pathways.
2. A Pathway will be an object that combines input points to be masked (shunted) for a set duration, and an output point to be activated, when a particular card receives a local grant at a reader.
   a. For example, a Pathway will provide the capability to contain the motion detector inputs along the hallway path to the user’s office.
   b. It will have the capability to contain the output point for a green light above the door to the office.
3. When the user presents their valid card to enter the building, the input points along the pathway to the office will be masked and the output point activated.
4. If the user attempts to access any areas other than the Pathway, an alarm will be generated.
5. After a set number of minutes have elapsed, the input points will be un-masked and the output point de-activated.
6. The Pathway will have the capability to be de-activated before the elapsed time, if another card is configured to “stop” a Pathway in progress.
7. Systems that do not provide Pathway programming will be unacceptable.

S. Database Audit Log
1. The System will be capable of creating an audit log in the history file following any change made to the System database by an operator.
2. Each database item will be selectable to audit the “add”, “update” or “delete” activities of related to that item. The System will record:
   a. The date and time of the activity
   b. The type of activity (add, update, or delete)
   c. The user who performed the activity
   d. The workstation at which the activity took place
   e. What information was modified
   f. What the old value was
   g. What the new value was

T. Operator Log
1. The System will be capable of creating an Action log in the history file following actions performed by an operator. The System will record:
   a. The date and time of the activity
   b. The user who performed the activity
c. The workstation at which the activity took place
d. What activity was performed
e. What database item the activity was performed on
f. What database group the item belongs to

U. Alarm Routing

1. The System will be capable of defining routing groups that determine what event information will be routed to a user or class of users.
2. The System will support routing group rules to be assigned to users or user classes, including single or multiple groups.
3. Each item in the routing group will be associated with a time zone, which will control when the routing group is valid.
   a. For Example – a specific workstation will be a valid target for routing after 6:00 pm in the evening.
4. Events from a specific facility (Channel) will be routed to a different set of operators during the day.
5. Certain kinds of events will be routed to a different set of operators on the weekend.
6. The System will support alarm rollover, which will forward an event to another workstation if it has not been acknowledged within a specified timeframe.
7. Systems that do not support alarm rollover will be unacceptable.
8. Routing of events will be separated via the following classifications:
   a. The communication channels on which the event originates
   b. The type of event that is generated
   c. The workstations to which the event should be routed

V. Hardware Templates

1. The System will include the ability to define Hardware Templates (Door Templates) in order to simplify the process of creating an Access Control System.
2. Hardware Templates will allow a user to define a “typical” door configuration, and then use that template over and over in the process of defining doors.
3. Hardware templates will allow the user to create device types and device property settings, which are specifically designed for the special requirements of each type of access point or alarm input on each project.
4. The Hardware Template will allow the System operator to define a template for multiple separate doors made up of the same parts.
   a. For example a typical door may include: Card Reader, a Lock, a Door Position Switch, a Request to Exit Device, and a Local Sounder for “Door Held Open” alarms.
5. The System operator will have the capability to create a template defining the 5 different categories of components that make up the door (Device Types), set the default values for each of the components, define any Interlocks and / or Guard Tour parameters, and then use that template to create the multiple separate doors.
6. By defining the component types and their default values within the template, the user will greatly reduced the overall amount of time
necessary to add a door to the system.

7. An unlimited number of templates will be supported, allowing a user to pre-define every type of door configuration within a particular facility.

8. Once the templates have been defined, the process of building doors will be quick and simple.

9. All Inputs and Outputs will have no pre-defined or fixed functionality and will be programmable for any functionality the user desires.
   a. For example, an Input point normally reserved for use as a Request to Exit should be capable of being re-programmed for any other desired functionality if a Request to Exit device is not required.
   b. Systems that do not provide this capability will be unacceptable.

10. Modifications can be made to templates after creation, where users will have the ability to select if the changes are to be applied to existing logical devices using the resource buttons Yes, Yes to All, No, and No to All.

W. Access Control Functional Requirements

1. Functions will include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of card/PIN, card, and video.

2. The following features will be programmable and will be capable of being modified by a user with the proper authorization:

X. Time Zones

1. Will define the period during which a reader, card, alarm point, door, or other system feature is active or inactive.

2. In addition to Monday — Sunday, there will be at least one day of the week called Holiday.

3. The following requirements will apply:
   a. Time Zone name: Will be at least 24 characters.
   b. Time Zone description: Will be at least 40 characters.
   c. Start time: Will define when the time zone becomes active.
   d. Stop time: Will define when the time zone becomes inactive.
   e. In use box: Will be used to activate the defined time period.
   f. Check off boxes: Will be provided for each day of the week including at least one holiday.

Y. Holidays

1. The application will allow holidays to be entered into the System.

2. Holidays will have a start-date plus duration defining multiple days.

3. Holidays will have a holiday type of 1, 2, or 3, which may be defined by the user.
   a. For Example Type 1 may be standard holidays, Type 2 may be half-day holidays, and Type 3 may be holidays for factory facilities only.

4. The time zones defined for the holiday type will be used in place of the
normal time zone for the day on which the holiday falls.

5. The following requirements will apply:
   a. Holiday name: Will be at least 24 characters.
   b. Holiday description: Will be at least 40 characters.
   c. Date: Will be the date the holiday falls on.
   d. Type: Will define holiday type 1, 2, or 3.

Z. Response Codes

1. The system will allow the user to enter a pre-defined code to represent a
   response to an alarm occurring in the facility.

2. The following requirements will apply:
   a. Response code name: Will be at least 10 characters.
   b. Response code message window: Will allow “free flowing” text to
      be entered up to 255 characters.

AA. Clearance Codes

1. The system will allow the user to establish groups of readers at a facility
   for the purpose of granting or denying access to badge holders.

2. Clearance codes will be assigned to individuals, and may be modified for
   individual users in the Badge holder Maintenance application.

3. The following requirements will apply:
   a. Clearance code name: Will be at least 12 characters.
   b. Clearance code description: Will be at least 40 characters.
   c. Default Time Zone: Will be selectable for a reader when added to
      this clearance code.
   d. Select Time Zone: Will be selectable for the reader from a combo
      box if the default time zone is not desired.
   e. Search: The System will be capable of searching by a reader
      description or location and have the ability to define search
      criteria.
   f. Clearance Code Reader List window: Will display the selected
      readers and time zones.
   g. Added or deleted readers: The System will provide a window
      indicating the number of cards that must be downloaded when a
      reader has been added to or deleted from a clearance code.
      1) This window will also have provisions to download the
         cards immediately, later, or not at all.
      2) The download later function will provide a means to
         schedule the time and date the download should occur.
   h. Clearance code download schedule: Will allow the user to
      download the data at a later time and schedule a date and time.
      1) The dialog box will include the date, time, and number of
         cards.
      2) It will also be possible to edit or remove the date and time.
   i. The System will provide the ability to create clearance codes that
      can have predetermined automatic expiration.
      1) The Clearance Code screen will provide a checkbox to
         select “Never Expires” if the selected time zone will always
         remain in effect.
2) The “Expires In” checkbox will be selected to define the amount of time in which the clearance code time zone will expire.

3) The System will provide two text boxes, which define the expiration designations.

4) The first text box will define the number and the second text box will define the time increment from a drop down list including Days, Hours, or Minutes.

5) For Example, if the number 2 is entered in the first text box and Days in the second text box, the clearance code time zone will expire in 2 days.

BB. Group Access

1. The System will allow a user, or group of users via Company selection, a temporary GRANT or DENIAL of access to specific readers or areas based on a pre-configured Event.

2. The Group Access function will limit access to a group of cardholders, overriding all other access criteria.

3. The Group Access will have a start and stop time/date along with the assigned Logical Devices (Type Door).

4. The System will support Multiple Logical Devices (Type Door) to be assigned to one Group Access Project.

5. A Group Access Project will be assigned to a card on the Card Information Screen of the Badge Viewer.

CC. Events

1. The Event Maintenance application will control processing done at the host computer that allows the user to associate nearly any input (trigger) with almost any sequence of outputs (actions) that the system is capable of executing.

2. A trigger may be a single “input” or any number of “inputs” that need to occur before an action is executed.

3. Actions will be executed in the order of their user programmed sequence number.

4. The following requirements will apply:
   a. Within the Event Maintenance application, the user will be able to:
      1) Add event names: Names will be up to 40 characters.
      2) Select event type: Will be selectable from the Event Type Maintenance application along with an event description of up to 40 characters.
      3) Define event triggers: Event triggers will be defined to indicate when the required trigger input must be used. Drop boxes will provide information from previously defined fields.
         a) Trigger Type: Will indicate how often the trigger may occur in order to cause the event to happen. Choices will be “repeatable”, “once only”, or “disabled”. A once only event will turn to “disabled” upon event execution.
b) Reader ID: Will indicate the reader that must be affected to cause the trigger to occur.

c) Alarm Type: Will indicate the alarm type that would trigger this event.

d) Alarm Number: Will indicate the alarm number associated with the alarm that would trigger this event.

e) Card Number: Will indicate the card number that would trigger this event.

f) Date: Will indicate the date this trigger would have to occur for the event to happen.

g) Time: Will indicate the time this trigger would have to occur for the event to happen.

h) Group Code: Will display the group code associated with the group of doors or alarms that will trigger the event.

i) Clearance Code Cards: Will display the cards assigned this clearance code that will trigger this event.

j) Type of Transaction: Will display the type of transaction that would cause the event to occur.

k) Time Zone: Will indicate the time zone during which the trigger is enabled. No time zone will imply the trigger can occur at any time.

l) Company Code: Will indicate the company code that would cause the event to occur.

4) Define actions for the event: This function will be used to define the following: a) A sequence number for the action to be executed upon this event being triggered. Actions will be executed in the order of their sequence numbers. A list of valid actions will be provided. Choices will include, but not be limited to:

a) Override; unlock a reader or a group of readers.

b) Arm alarm, software level, or a group of alarms.

c) Arm input point or a group of input points.

d) Arm output point or a group of output points.

e) Shunt an alarm or a group of alarms.

f) Shunt an input point of a group of input points.

g) Shunt an output or a group of outputs.

h) Void a card.

i) Local Grant or pop a door open.

j) Issue alarm.

k) Run a program.

l) Issue a CCTV command.

m) Activate output point.

n) De-activate output point.

5) The command issued for the system to perform Parameters 1 and 2 will be from the event processor parameters.
1. Application will include the capability to create an unlimited number of customized alarm pages for the alarm monitor and each will be assignable to Users and User Classes.

2. The following information will be individually configured for each alarm page:
   a. Alarm description: Will provide a brief description of the alarm type.
   b. Default Window State:
      1) Normal: Alarm Page window will be sized to fit available area.
      2) Maximize: Alarm Page window will be maximized within the alarm monitor.
      3) Minimize: Alarm Page window will be minimized within the alarm monitor.
   c. Default Map: Will provide the capability to include a default Map in the Alarm page.
   d. Event Types: Will provide the ability to select the individual event types that are to be indicated as alarms. Physical events from the hardware (default events) will be associated with real-world events (event types), which can be tailored. The System will allow an alarm state on an input point to be associated with the event type, which is appropriate for the particular device to which the input point is actually attached.
   e. Alarm Columns: Will provide the ability to select the columns that will appear on the alarm page as well as the order in which they appear.

EE. Event Types

1. The following requirements will apply:
   a. Event type definitions: Definitions will be pre-shipped with system software but will be capable, upon installation, of being modified, added to, or deleted from the system.
   b. Event type maintenance application: Will allow the user to customize alarm color appearance, enter alarm text, or partition alarm types.
   c. Event type information: The following information will be included:
      a) Alarm name: Will indicate the name given to the alarm.
      b) Alarm description: Will provide a brief description of the alarm type.
   d. Re-issuance frequency: Will indicate (in minutes), how often alarms will re-issue if the alarm state continues.
   e. Global shunt status: Will indicate whether alarms are shunted, overriding the individual alarm shunt status, or are armed or shunted on an alarm-by-alarm basis.
   f. Auto clear field: Will indicate whether an alarm will be automatically cleared from the alarm monitor or “normal” operation for this alarm type will occur.
   g. Force note field: Will provide an indication to the user whether or not he or she entered an operator log comment when an alarm is received.
h. Return separate alarm box: Will indicate whether or not to treat the return to normal alarms as a separate alarm.

i. Default alarm message window: This message will be displayed on the alarm monitor if an alarm of this type occurs that does not have a custom alarm message.

FF. Dynamic Graphical Maps

1. The System will provide the user with the means to add maps and indicator icons to maps that will represent input/output points, logical devices, or cameras located throughout the System. System maps will display the state and condition of alarm points. The System will also provide the ability to monitor the channels or panels.

2. The System Map Builder will allow the user to graphically represent various resources such as logical devices on engineering floor plan drawings (maps). The drawings will be in DWG (Vector), WMF, or BMP (Raster) format to represent a map with a corresponding indicator icon detailing the input/output points, logical devices, or cameras. When an alarm occurs, the associated map will appear on the alarm monitor as a graphical interface and will indicate the state and condition of the alarm point. The System will allow multiple maps to be displayed at any single time.

3. The System will display maps created in AutoCAD. These AutoCAD drawings have defined layers for the separate elements within the enterprise map, which the user will be capable of viewing from the Layers dialog box. Layers will be able to be “frozen” or “thawed”.

4. The Layers dialog box will consist of three sections: a Layers List, Edit section, and Filters section. The Layers List will identify the layers within the selected AutoCAD drawing. The Edit section will include commands used in selecting and further defining layers. The Filters portion of the dialog box will provide options to determine filtering properties. Each map created in the Map Builder will contain icons that represent the resources associated with the System devices. The icons available for positioning on the alarm map will include Logical Devices, Groups, Maps, and CCTV Cameras.

5. The user will have the capability to add and edit a resource, display resource text, and cleanup a resource. The lower portion of the Map Resource dialog box will allow for the definition of the icon position within the selected map.

6. The horizontal placement will be defined by entering values in the Starting X and Ending X boxes. The vertical placement will be defined by entering values in the Starting Y and Ending Y boxes.

GG. Brass Keys

1. Will maintain information related to brass keys that are issued in the facility.

2. The following requirements will apply:
   a. Brass Keys Maintenance application: Will allow the user to view any existing information in the Brass Keys dialog box. A user, with proper authority, will be able to modify, add, delete, or partition
brass keys from the system software.

b. Brass Keys Maintenance will include, but not be limited to:
   1) ID number assigned to the brass key: Will be up to 40 characters.
   2) Type of brass key: Will be up to 40 characters.
   3) A description of the type of brass key: Will be up to 40 characters.

c. The ability to prevent the duplication of keys will be made available where users can disallow a key from being assigned to multiple users.

HH. Badge Holders

1. Will maintain information related to a Badge holder’s card access privileges in the system. Upon entering this application, a window will appear on the screen. All actions (add, modify, or delete) involving badges and cards will be initiated from this window. Access privileges will be as defined for the company that employs the Badge holder. Access privileges will be linked to the cards used to gain access to doors in the facility. Modifications will be made by adding or deleting clearance codes, or by door types assigned to the cards or to a Badge holder. The following requirements will apply:

   a. Badge Information window: This window will allow the user to search for Badge holders in the system that meet certain search key information. The badge information window will be divided into three sections:
      1) Top (Search Field) section: Will select the fields that will be returned in the search results area.
      2) Middle (Search Key) section: Will initiate a search for badge or card records.
      3) Bottom section: Will list the results of a search.

   b. In the Badge holder Maintenance application, the following will be minimum requirements:
      1) Add new badges: Information will be entered onto the Badge Info property sheet, displayed on the Badge Maintenance dialog box. The fields displayed on the Badge Info property sheet will be related to general Badge holder information and will include:
         a) Badge Number: The unique badge number will be up to 15 digits.
         b) Issue Date: Will be the date the badge was issued.
         c) Expiration Date: Will be the date the badge expires.
         d) Badge Type: Will be as defined by System Administrator.
         e) Badge holder Last Name: Will be a minimum of 40 characters.
         f) Badge holder First Name: Will be a minimum of 20 characters.
         g) Badge holder Middle Initial.
         h) Company: The Badge holders Company will be selected via the search mechanism.
i) Photo ID Enrollment and Image View.

j) Signature Capture and Signature View.

2) The System will also be capable of accepting up to ten (10) user-defined fields containing at least 25 characters to the property sheet.

3) User Defined property sheet: A tab will be definable and contain up to 20 definable fields containing up to 40 characters. The property sheet label and the data fields will be defined in the control record under system hardware.

4) Assigning cards: Each card that is assigned will be defined to a badge, and will possess the access privileges of the company to which it is assigned. Card information dialog box: Will include, but not be limited to the following:
   a) Unique card number between 1–15 digits in length.
   b) Badge type as defined in the Badge Maintenance application.
   c) The company code associated with this particular card. The card will take on the default access/clearance codes for this company.
   d) Date the card is issued.
   e) Date the card will expire will include month, day, and year.
   f) Last date and time the card attempted access.
   g) Door ID of the last door the cardholder attempted to access with this card.
   h) The status of this card, which may be selected from a drop box. Selection will include at a minimum active, disabled, expired, lost, stolen, terminated, unaccounted, or void.
   i) It will be possible to grant executive privilege for this card and allow it to:
      (1) Obtain a valid access at any reader on the node.
      (2) Override doors.
      (3) Download this card information to the panel.
      (4) Issue a trace alarm whenever the subject card is used; however, access will not be denied.
   j) Issue level (0-15): For systems using a magnetic stripe card with an issue number field, the issue number of the card will indicate how many times this card has been issued.
   k) In, out, or undefined (In-X-It status): Will provide a status indicator of a card utilized on specific hardware.
   l) PIN code: Will be provided if card and keypad number are required for high security. The PIN code will support up to 8 digits. The System will also support checkbox to issue random PIN codes.

   c. Card Information property sheet: Will display information related to the cards assigned to a Badge holder. The badge number and
Badge holders name will appear in the section labeled cards, and any cards that are defined will appear below the badge number, forming a hierarchical list below the Badge holder's name. The information included on this hierarchical tree will appear in the following order:

1) Badge number – Badge holders name
2) Card one – Clearance codes and door codes
3) Card two – Clearance codes and door codes

d. Brass Keys: Will be assigned to Badge holders on the Brass Keys property sheet on the Badge Maintenance dialog box. When added, they will appear on the brass key list on the property sheet. Brass Key property sheet will include, but not be limited to the following:

1) Issue date
2) Due date
3) Return date

e. Company Information: Each badge defined in the system will be associated with a company.

II. Badge Manager

1. The Badge Manager will allow users to quickly assign an access card and badge record in Pro-Watch. This wizard will not be an all encompassing wizard as only the basic required fields will be taken into account when using this wizard. The wizard will allow users to add a card to the system based on Company driven clearance codes with four entry field and less than 7 total clicks. The overall goal from a time to program standpoint is to offer a solution where a new badge holder and card record can be completed down to less than 30 seconds by using this wizard.

2. The wizard will be made available from the main Welcome Wizard as well as by right clicking on the listing of active badge records in the main listing on the left hand side of the badge window. When performing a right-click, the user will see a selection window appear that will state “Create new Record”. When selecting this option, the Badge Manager Wizard will appear and guide the user through a record entry.

JJ. Video Image / ID Badging System

1. The System will include seamlessly Integrated ID Badging System/Video Image System.

2. Badge Fields
   a. The System will provide a minimum of 37 default badge fields. Each field will be displayed in a grid in which the each of the attributes of the field is displayed in a separate column.
   b. Fields marked as “True” in the User defined field will have the capability to be deleted as desired; those marked “false” will be system fields will not have the capability to be deleted. The System operator, that has been granted proper System permissions, will have the capability to view, add, edit, and delete badge fields.
   c. Badge Field Properties:
1) Column Name - Descriptive column name.
2) User Defined - Will display True when adding a new field. This is not user definable.
3) Display Name - Name applied to field when it is assigned to a Badge Page.
4) Allow Nulls - This check box is only activated if Date, Date time, or Time Data Types are selected. When checked it allows the field to contain null values.
5) Data Type - Select the data type appropriate to the data the field is intended to capture the choices are:
   a) Auto-increment - When selected this field is automatically incremented to the next highest integer, it starts with the number entered into the “Auto Increment Start” Field under Auto Increment Options.
   b) Blob - Select to display an associated blob type. Note - This data type will be displayed only if there exists on the system a blob type, which is not already assigned to a badge field and the resource type assigned to that Blob Type is not Badge Types.
   c) Bool – The bool (Boolean) is a Data Type checkbox, which the user will be able to choose to indicate a true or false (yes or no, “1” or “0”) condition for a badge field.
   d) Date - Select to create a date field.
   e) Date time - Select to create a date/time field.
   f) Int - Select to create an integer field.
   g) Money - Select to create a field, which will display and store monetary values.
   h) Resource - Select to create a field to hold a resource. A resource can be any item represented by an icon under the Database Viewer.
   i) Short - Select to create a field, which can hold an integer from 0 to 67,535
   j) Time - Select to create a time field.
   k) Userdefined – Selection of this datatype will create a pick list from which the badging user can select predefined values. The System will support Badge Field pick-list definitions. For example: Badge Eye color Pick-list may be user defined to include brown, blue, green, hazel, gray, etc. The values are defined by selecting the “Edit User Defined Values” button.
   l) Varchar - Select this option to define a text data field.
6) Indexed - Select true to create an index on the selected field. This may be desirable if searches are conducted on the selected field. This is not available on Boolean fields.
   a) Unique - Select true to require all entries into the selected field to be unique.
b) Data Size - This can only be set for Varchar fields, values can range from 1 to 4000.

c) Resource Type - If the resource data type is selected this field is activated allowing the user to select from the available resource types.

d) Blob Type - Found under Blob Options, this field is activated when Blob is the selected data type. Select the desired Blob Type from the drop down list.

e) Blob Text - Also found under Blob Options, controls the display of the label on the select Blob Type. The choices are - Don’t display, Display on Top or Display on Bottom.

f) Auto Increment Start - Found under Auto Increment Options, this is activated when the auto-increment data type is selected. Defines the starting point for the newly defined automatically incrementing field.

KK. Badge Designer

1. The Badge Designer will allow the user to edit or create new front and back badge design layouts.

2. The System will be provided with default “Contractor” or “Standard Employee” badge designs.

3. The user will be able to add several types of Badge Designer items by clicking the appropriate button from the corresponding tool-bar.

   a. The toolbar buttons will include:

      1) Save: Saves Badge Designer settings.
      2) Exit: Exits from Badge Designer.
      3) Idle: Selects one or more Badge Designer items.
      4) Place Text: Inserts text into Badge Designer.
      5) Place Bitmap: Inserts bitmap image into Badge Designer.
      6) Place Photo: Inserts photograph into Badge Designer.
      7) Place Barcode: Inserts bar code into Badge Designer.
      8) Place Shape: Places shape into Badge Designer layout.
      9) Place Signature button—use this button to place a signature into the Badge Designer layout.
     10) Change Layering button—choose this button to open the Badge Item Layering dialog box.
     11) Select Next Item—click this option to select the next Badge Designer item Badge Designer layout.

   b. Badge Designer Measurement Properties: This option will allow the user to define the Badge Designer ruler to use inches or millimeters.

   c. Badge Designer Zoom Factor: This option will allow the user to zoom to 200%, 100%, 75%, 50%, 25%, Fit to Window, and Custom.

   d. Grid Settings: The System will allow the user to display a grid on any badge design, determine the density of the badge design grid, and align selected badge objects to align to a grid.

   e. Badge Designer Block-outs: The System will allow the user to
define an area of a badge that is “blocked” from the print area. A block-out will be utilized to prevent the printing onto a certain section of a card, such as the magnetic stripe or smart card chip.

f. Badge Designer Properties: The user will have the capability to define all the properties of each Badge Designer item. The user will have the capability to establish the color properties of signatures and bitmaps or choose the types of shapes to add, such as lines or rectangles.

4. Bar Codes
   a. The System will support data from the badge field database to be linked directly to the record holder and visible in a barcode output. The barcode will have the ability to span multiple fields and will allow support for the following types of barcode formats:
      1) 2of 5
      2) 2 of 5 Interleaved
      3) 3 of 9
      4) Codebar
      5) Code 39
      6) Code 93
      7) Code 128
      8) EAN 128
      9) EAN 13
     10) ITF
     11) MSI
     12) Code 11
     13) Code B
     14) Telepen
     15) UPC A
     16) UPC E
     17) Code 128A
     18) Code 128B
   b. The System will provide a dialog box allowing the user to select all that apply:
      1) Show Text: this option shows the barcode data in text, below the bar code.
      2) W Bearer Bar: this option will display the width bearer bars (top and bottom borders).
      3) H Bearer Bar: this option will display the height bearer bars (left and right borders).
      4) Check Digit: this option will provide for error checking.
      5) Show Spacer: this option will display the space before and after the barcode data.
      6) Switch Text: this option will switch the top and bottom text.
      7) Check Digit 2: this option will provide for error checking.
      8) Arial: this option will designate the text font type.
      9) Courier New: this option will designate the text font type.
     10) Bold: this option will designate the text font type.
     11) Italic: this option will designate the text font type.

5. Photograph Properties
   a. The System will allow the user to define the Photo Index and enter a value between 1 and 99. This value will correspond to the index
setting of the photograph blob type. This value will determine which photograph will be printed on the badge if the badge holder has more than one photograph associated with their record.

b. The System will allow the user to “Stretch Width” to automatically stretch the width of the photograph to fill the display box on the badge.

c. The System will allow the user to “Stretch Height” to automatically stretch the height of the photograph to fill the display box on the badge.

d. The System will allow the user to select “Keep Aspect Ratio” to keep the ratio of the width of an image to its height; thus, avoiding distortions.

e. The System will provide a Ghosting section of the dialog box and will allow the user to move the scroll bar indicator to the desired effect.

f. The System will allow the user to choose the badge orientation for Portrait or Landscape. The System will allow the user to choose the option to Print Both Sides if the printer supports duplex printing (printing on both sides of the card).

6. Layering Badge Items

a. The System will allow the user to properly layer badge layout items within a selected layout.

7. Badge Profiles

a. The System will allow the user to add, edit and delete Profiles that establish control information for the Access Page, Partition Page, Assets, and searchable card fields.

b. Profiles will include an Auto Disable Card function, which automatically voids a card, if a defined time frame has elapsed without a card read.

c. The System will allow the user to design the layout of personnel record views, with the capability of creating multiple views for assignment to operator classes, for display of selected fields in the database.

d. Badge fields will be user definable and will not be limited in the number or type of fields, providing the user flexibility to create and delete fields as the requirements change for each location.

e. Multiple graphic fields will be supported to display photos of the badge holder, cars, and/or assets as well as scanned documents.

f. The System will provide programmable defaults for badge profiles allowing the user the ability to set a default value for each field placed on a page when building a badge profile.

g. The user will have the capability to program required fields to make badge profile creation consistent throughout the System, automating the data entry for common types of badge information.

8. Copy Card Function

a. The Copy Card function will provide the user the ability to automatically recreate clearance codes and all other data (user level, expiration, special access, etc.) on the card record to a new card.

b. The user will have the capability to choose copy, and all significant card information will be ‘memorized’ and is used later, during the
paste operation.
c. The paste function will work from the state of the card at the time of the copy, not at the time of the paste.

a. The System badging module will include progressive search engine that will allow the operator to quickly pinpoint any information in the badge record.
b. This search will provide the capability to be performed on any user-defined field that exists in the badge record.
c. The System will utilize .NET technology and full text indexing; the search criteria will efficiently target the required data while using a minimal amount of system resources.

LL. Users
1. Will maintain information related to the users of the system software, i.e., and the individuals who have access to the database.
2. Users entered into the system will take in the access privileges of the class to which they are assigned.
3. The following requirements will apply:
a. Defining users information: When defining users, it will not be necessary to modify information related to alarm types, programs/functions, workstations, alarm pages, alarm toolbar, and partitions unless it is necessary that the user's privileges be different from those of the user's class.
b. Modifying user information: Information related to a user will be modified on dialog boxes, which are accessed from the Main User Maintenance dialog box.
c. User Maintenance application: Will allow a user to be added, modified, partitioned, or deleted. User information will be in addition to that defined for the user's class. This information will include, but not be limited to the following:
   1) ID name: Will be at least 10 characters.
   2) Class: Selection of the class assigned to the user.
   3) User's last name: Will be at least 40 characters.
   4) User's first name: Will be at least 40 characters.
   5) Badge number: Valid badge number assigned to the user.
   6) Expiration date: Date the user ID expires.
   7) Alarm types: Will indicate a user's alarm.
   8) Add programs/functions: Will allow additional programs and functions to be added to a user.
   9) Add workstations: Will allow additional workstations to be added to a user.
  10) Add alarm page: Will allow additional alarm pages to be added to a user.
  11) Modify alarm toolbar: Will allow the toolbar to be modified for a user.
4. All inaccessible resources will be hidden from the user's view.
5. Users that have limited permission sets will not be able to see resource selections they have not been assigned permission to access in the Database Configuration viewer.
6. The system will incorporate the use of a Permission Manager.
   a. This will be used for the creation and assignment new users to the system.
   b. The Permission Manager will take advantage of the existing permission classes.
   c. It will be made available to users through either the shell entry manager or by right clicking in the User workspace and selecting ‘New’.
   d. When new is selected the user will be prompted if they would like to utilize the Permission Manager.
   e. If the user answers ‘Yes’, then they will be shown the windows outlined below.
   f. If the user answers ‘No’, then they will be given a standard unpopulated class record for user entry.

MM. Reports

1. The reporting module will provide a HTML style of operation and be self-contained within the System application.
2. The reporting module will provide a split screen where the upper portion will display the standard report, while the lower section will show the search criteria.
3. The report preview will be provided in a separate viewer window and allow for scheduling, exporting, and printing of reports.
4. The System operator will be allowed to save reports to their profile and have them available through ‘Quick Tasks’.
5. The Quick tasks will be displayed on the right side of the screen at all times and will be customizable per user/user group.
6. The Reports toolbar will provide icons which enable the System operator to preview a report, print a report, export a report, add to “My Reports” folder, schedule a report, add a custom report, and clear selection criteria data.
7. The Export Report button will enable the System operator to export any report as delimited text, an Excel spreadsheet, an Adobe PDF, rich text format, and HTML.
8. The standard reports that will be included with the System:
   a. Access Reports:
      1) Badge holder Access to a Logical Device
      2) Card Status
      3) Clearance Code/Badge Access
      4) Last Access at a Logical Device
      5) Last Access by a Badge Holder
      6) Logical Device Access by a Badge holder
      7) Mustering
   b. Badge holder Reports
      1) Area Attendance
      2) Badge holder Detail
      3) Badge holder Summary
      4) Key Assignment List
   c. Company Reports
      1) Company Clearance Code
2) Company Summary

d. Configuration Reports
   1) Badge Profiles
   2) Badge Types
   3) Brass Key List
   4) Channel Configuration
   5) Classes
   6) Clearance Codes
   7) Database Tables
   8) Device Types
   9) Dialup Schedules
  10) Event Points
  11) Event Procedures
  12) Event Types
  13) Guard Tours
  14) Hardware Classes
  15) Hardware Templates
  16) Logical Devices
  17) Modem Pools
  18) Panel Types
  19) Partitions
  20) Printers
  21) Response Codes
  22) Routing Groups
  23) Time zones
  24) Workstations

e. Logging Reports
   1) Database Audit Log
   2) Compliance and Validation
   3) Event Log
   4) Operator Log

f. User Reports
   1) User Detail Report
   2) User Summary Report
   3) User Group Report
   4) User Group Summary Report

9. The System will provide reporting capability for printing of selected system transactions from the disk files by specific time and date selection, range from time and date to time and date, or from start time to end time each day of the selected date range.

10. Provide feature to generate a history report for an alarm point(s) state. An alarm point state will be defined as Normal, Alarm, Trouble, or Ajar.

11. Provide feature to generate a history report of system alarms. A system alarm state will be defined by panel and include any of the following information: communication, ground fault, power, panel reset, low voltage, panel tamper, and loop communication.

12. Provide feature to generate a history report for a card(s) state. A card state will be defined as Normal, Trace, Not Found, Anti-Passback Violation, PIN Violation, Time Zone Violation, Site Code Violation, or Expired card. Additional search criteria will include cardholders that meet
up to at least 3-note field restriction and filter the report with defined reader location(s).

13. Provide feature to generate a history report for system operator activities. Activities will be at least, but not limited to, acknowledged transactions, database file modification, and comments made to alarm events.

14. Provide complete database reporting of all data programmed into the system data files.

NN. Tape Backup

1. The System server(s) will utilize a tape backup system for backup and archiving capabilities.
2. The System will allow the user to perform backups at pre-determined times including hourly, daily, weekly, and monthly intervals.
3. The System will also support differential database backup.
4. A differential database backup will record only those data changes made to the database since the last full database backup.

OO. Archiving

1. The System will allow system operators to archive information to a backup source.
2. The System will provide table maximum alerts, which will notify users of the size of their database.
3. The system will provide an archive feature, which supports a start date and end date of information to be archived with the following options:
   a. Archive only — this option will archive the designated event records defined by start and end times.
   b. Archive and Purge — this option will archive the designated event records and the purge them from the system.
   c. Purge only — this option will remove the event records from the system.
   d. Restore — this option will restore previously archived event records.
   e. Abort — this option will abort a restore/archive action.

PP. Data Transfer Utility

1. The System will provide a data transfer utility that will make the importation of information to the System database efficient and accurate. Each data source will be defined as a Profile in the Data Transfer Utility. A profile will define all aspects regarding how the data will be loaded to the System, including the type of data load, where the data comes from, the type of logging, and the mapping between the System and the data source.
   a. The System will provide option buttons to specify a data source:
      1) Delimited: - data in a text file, individual fields separated by vertical bars, commas or tabs.
      2) Fixed: - data with a fixed length will allow import but cannot export fixed length data.
      3) SQL server native database driver
4) **ODBC (Open Data Base Connectivity):** an Application Programming Interface (API) that allows import from and export to a database.

5) **LDAP (Lightweight Direct Access Protocol):** an Internet protocol that will allow import from and export to a database.

6) Images - allows export but cannot import images as data.

b. The Profile Description tab will allow at a minimum, definition of:

1) Profile ID, which includes unique profile ID used to identify the profile.

2) Profile Description

3) File Delimiter, which defines the text character that separates the data fields in the delimited data file. The System will provide a drop-down list:
   a) I-Vertical Bar
   b) Comma
   c) Tab

4) Text Qualifier. The System will provide a drop-down list for delimited database text qualifiers:
   a) <None>
   b) Double Quote { " }
   c) Single Quote { ' }

5) Download access changes to Panels. The user will select this check box to download the changes to the respective panels, only if access has changed.

6) Data File Key Column #. This will be the delimited field number in the delimited file that is used to determine whether a record will be an Update or an Insertion or the Start and End column numbers of the fixed-length key field.

7) System Key Identifier. This is the System data field that maintains the keys of the external system. This will be used to determine if a record will be an Update or Insertion.

8) System Database Location. This will display the read-only fields that will be enabled when a System Key Identifier is entered. The first field will display the name of the database table and the second field will display the name of the database column in that table to which the data will be transferred by DTU.

9) File Transactions. The type of transactions this profile will contain. The System will provide the following option buttons:
   a) Insert Only: If a “Data File Key Column #” will be provided, the DTU will only insert a new badge record if the key column value is not found. An error will be displayed in the log file if an existing badge record is found. If no “Data File Key Column #” is provided, every record will be inserted into the System.
   b) Updates Only: The DTU will use the “Data File Key
Column # to look for the matching System record. An error will be logged in the log file if the badge holder is not found in the System database.

c) Inserts, Updates: The DTU will use the “Data File Key Column #” to look for the matching System record. If a matching record is not found, the DTU will insert the data. If a matching record is found, the record will be updated.

10) Communications Server. This will be the name of the System server to which the data will be loaded.

11) Database Server. This will be the name of the System database to which the data will be loaded.

12) Database Name. This will be the name of the database.

c. In addition, depending upon the data source type, additional tabs will be provided to configure the import procedure:

1) Data files tab will provide the location of the data source and option buttons for which files are desired to be loaded, including: Load all files in Directory Load only the file with the following name Load all files that match the following naming pattern: selecting this option will load all the files that match the specified naming pattern. Wildcard “**” and single character wildcard “?” will be used to specify a naming pattern.

2) Logging tab will allow the System to generate a log file for scheduled data transfer sessions, including email configuration.

3) Data Mapping tab will allow the configuration of mapping rules. Mapping rules determine how each column value in the external database will be converted into a System column value. For example, one mapping rule could be “whenever you see the value ‘123’ for Department_ID, map it as ‘Human Resources’ when importing the record into the System.”

4) Remote Data Tab will define where the data source is located and defining the Key Locator to determine if a record is an Update or Insertion.

5) Images tab will allow for JPEG photo import and defining location and image naming sequence.

6) Manual Load tab will allow the user to load a sample data file to the System. After a sample data file is loaded, the icon for all rows will display as a black arrow. The icons will change to a green circle if the sample data is loaded successfully to the System or a red circle if there was an error in loading the data. The System will display the reason for the failure by double-clicking on a row with a red circle.

d. The System will also support data exports to synchronize the System with other systems that it needs to interact with. Such synchronization will be easily accomplished by making the necessary edits in the System and then exporting the edited data to the external database.
QQ. Generic Channel Interface

1. The System will provide the ability to define generic communications channels over serial port or TCP/IP network socket including IP address and port/socket, to support custom integration of external foreign devices.

2. The System will generate events based on data received from the channel matching operator pre-defined instructions.

3. The System will allow the user to define a Channel Description and provide an “Installed” checkbox.

4. The System will allow Channel Definition as follows:
   a. Channel Type drop down list will include “Generic”.
   b. A “Generic” channel will have no sub-hardware.
   c. A “Generic” channel will support serial ports and TCP connection methods.
   d. A “Generic” channel will provide the following tabs:
      1) Define Channel Information
      2) Communications
      3) Parameters
      4) Events
      5) Partitions

5. The user will have the capability to define:
   a. Geographic time zone from a drop down list.
   b. Attempts - which will define the number of times the server will try to communicate with this channel before an alarm is generated.
   c. Poll Delay (ms), which will define the number of milliseconds between each poll cycle.
   d. Communications Break, which will define the number of poll cycles that will occur between each communication break test. A communication break will be a random sequence of characters sent across the channel to test the line connecting the device and the server.
   e. Spool Directory, which will be enabled only after a Log Printer Channel is configured. Path will be displayed when the Log Printer Channel is edited.
   f. Poll String will be enabled to poll an unsupported hardware device. The required Poll String for the unsupported hardware device will be found in the associated Technical Manual.

6. The user will have the capability to define inbound messages in the standard event definition screen to define the translation string from the generic device.
   a. The translation string will be a string of ASCII and control characters, which act as triggers for the event when detected in the input stream.
   b. The user will utilize a standard event procedure to define outbound messages, such as an acknowledgment back to the generic device.

RR. Event Manager

1. The system will utilize an event manager as a component of system
administration and offer the ability to have users control the amount of data stored as well as a quick snapshot of the logged data in the system.

2. Using the various logs in Event Manager, the user will be able to gather information about events, auditing, and operator actions.

3. The logs are defined as follows:
   a. **Event Log**
      1) The event log contains events logged by the application and events from within Pro-Watch.
   b. **Audit Log**
      1) The security log can record security events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.
   c. **Unacknowledged Alarms**
      1) The Unacknowledged alarms log will allow users to control items that are currently being dumped into the UNACK_AL. The ability to control what data is being inserted is important as a large majority of customers are not utilizing the alarm monitoring functionality. The ability to have the information easily truncated will be advantageous for smaller MSDE systems where database size limitations exist.
      2) A new resource will be placed on the left pane of the Administration Viewer. When clicking on the Event Manager dialogue (or icon), the tree will expand to show the various logs within the Event Monitor. The logs that will be available initially will include Audit, Event, and Operator. Highlighting any of the three options will result in a listing of data for the appropriate log in the right pane viewer. Right clicking on any of the resources will allow the following options:
         a) **Save Log**
            (1) This will allow the user to save the information in the log as a text (txt) file and the path for the file save will be user definable.
         b) **Clear All Events**
            (1) This will allow the user to clear all of the events that are in the view, prior to executing the clear, a dialogue box needs to warn the user that this action will remove the events from the database, as well as recommend that the data should be archived prior to deletion. If the user wishes to acknowledge the message and clear the log, a secondary box will appear re-confirming the deletion.
c) Properties
(1) This option will allow the user to program the size for the log size as well as program auto purging of events. The log size will be user definable selection, which will act as a trigger for purge options. The purge options available are defined as follows:
   (a) Overwrite when needed
   (b) Overwrite events older than ‘x’ days. The number of days will be user selectable.
   (c) Do not overwrite; this will require the user to manually purge the events.

SS. Server
1. Rack mounted enclosure
2. Duo Core Intel® Xeon® 5148LV processor, 2.33 GHz, 1333 FSB
3. 16 GB RDRAM
4. PERC 5/I, x8 Backplane, Raid10 controller
5. 1.8 TB HD Storage
6. Redundant Power Supply
7. 10/100/1000BaseT Network Interface Card
8. Remote access card
9. 24X CD-RW/DVD ROM Drive

TT. Workstation
1. Desk Top or Tower Enclosure
2. Duo Core Intel® Xeon® 5160 processor, 3.0 GHz, 1333 FSB
3. 4 GB RDRAM
4. PERC 5/i controller
5. 146 GB SCSI
6. 48X CD AND 48X CD-RW/DVD Combo
7. nVidia Graphics Card, with:
   a. 256 Mb graphic memory
   b. PCIe x16 interface
   c. Quatro FX 3450
   d. Dual VGA
   e. Associated cables
8. Integrated Audio
9. Speakers
10. 10/100/1000BaseT Network Interface Card
12. Monitors:
   a. Two (2) 20” LCD-TFT displays
   b. Adjustable dual display stand

4.03 ACCESS CONTROL AND ALARM DETECTION

A. Controller Panels
1. The security management system will be equipped with access control field hardware required to receive alarms and administer all access granted/denied decisions.

2. All field hardware will meet UL requirements. The supported field hardware will include, but not limited to, the following components:
   a. Intelligent Controller
      1) The IC will link the security management system software to all other field hardware components (card reader modules and input and output control modules). The IC will provide full distributed processing of access control and alarm monitoring operations.
      2) Access levels, hardware configurations, and programmed alarm outputs assigned at the administration workstation will be downloaded to the IC, which will store the information, and function using its high-speed, local 32-bit microprocessor. All access granted/denied decisions will be made at the IC to provide fast responses to card reader transaction. The System will provide the user the capability to query the IC to get a snapshot of memory availability, stored transactions and events, etc.
         a) IC Networking - The System will include a network-based interface module. The module will be a 10 MBPS Ethernet-based and capable of residing on a local area network (LAN) or wide area network (WAN) without connectivity to a PC serial port. The IC network interface module will be able to communicate back to the database server through industry standard switches and routers.
         b) Off-line operation - In the event that the IC loses communication with system software, it will continue to function normally (stand-alone). While in this off-line state, the IC will make access granted/denied decisions and maintain a log of the events that occur. Events will be stored in local memory and uploaded to the system software after communications are restored.
         c) IC Features
         d) Communications - The IC will include a primary and a secondary port for the purpose of communication to the host computer. The following communication formats will be supported:
            (1) RS-232 at a speed of 38.4 KBPS
            (2) RS-485 at a speed of 38.4 KBPS
            (3) Ethernet at a speed of 38.4 KBPS (10baseT, RJ45)
         e) Memory - Real time program updates and overall host communications will utilize flash memory. The standard IC will accommodate a card database of 7,800 cards, and a standard transaction buffer of 5,000 transactions. The memory expansion module will accommodate a card database of 157,000
f) Additional ports - Will be provided for connecting card readers and data gathering panels via RS-485 multi-drop wiring configuration. Each IC will support up to a combined total of 32 boards connected in any combination.

g) Devices - Up to 32 devices consisting of reader interface modules, alarm input modules (AIM), and relay output modules (ROM) will be supported. The devices will be connected in any combination.

h) Processor - The IC will contain a 32-bit processor.

i) Readers Capacities – Reader functionality and connectivity will be achieved through reader modules, and not directly to the IC. The IC will however support at a minimum the following:

1. Up to 8 card formats and facility codes
2. Multiple card technologies
3. Biometrics interface support
4. Smart card interface support
5. Integration with other manufacturers’ card readers
6. Issue code support for both magnetic and Wiegand card readers
7. Up to 8 digit PIN codes.

j) Redundant Communication - The System will provide a redundant or secondary means of communications with System Intelligent Controllers configured on a communication Channel. A Channel provides the connection between a regional/local server and a panel or hardware device. The System will support various types of channels to support numerous hardware devices, however, only a System Intelligent Controller will be configurable for Redundant Communications Support. If the primary method of communications fails, the System will automatically switch over to the secondary method. The possible primary/secondary combinations will include:

1. TCP/Dial Out
2. TCP/TCP
3. TCP/Hardwired
4. Hardwired/Dial Out
5. Hardwired/TCP
6. Hardwired/Hardwired.

k) Electrical Power - Primary input power will be 12VDC +/- 10% @ 400mA with an operating range of 10 VDC to 16 VDC. The IC will be equipped with an uninterruptible power supply (UPS) and backup battery.

b. Single Reader Module (SRM)
1) The SRM will provide an interface between the IC and the card readers. The SRM will operate with any card reader that produces a standard Wiegand (Data 1/Data 0 or Clock and Data) communication output. A single IC will be able to multi-drop up to 32 SRMs on four separate RS485 ports. The following requirements will also apply:
   a) Up to 32 SRMs will be connected to each IC, distributed across the four RS485 ports.
   b) Each SRM will include two (2) supervised inputs and two (2) relay outputs.
   c) Up to 8 unique card formats will be supported.
   d) The SRM will support an integrated card reader/keypad.
   e) The SRM will support three (3) access modes upon loss of communication with the IC. These modes will be locked, unlocked, or facility code.
   f) Input power will be 12VDC +/- 10% @ 400mA with an operating range of 10VDC to 16VDC.

c. Dual Reader Module (DRM)
1) The DRM will provide an interface between the IC and the card readers. The DRM will operate with any card reader that produces a standard Wiegand (Data 1/Data 0 or Clock and Data) communication output. A single IC will be able to multi-drop up to 32 DRMs on four separate RS485 ports. The following requirements will also apply:
   d) Each DRM will support two card readers, each of which may be up to 500 feet from the DRM.
   e) Up to 32 DRMs will be connected to each IC, distributed across the four RS485 ports.
   f) Each DRM will include eight (8) supervised inputs and six (6) relay outputs.
   g) Up to 8 unique card formats will be supported.
   h) The DRM will support an integrated card reader/keypad.
   i) The DRM will support three (3) access modes upon loss of communication with the IC. These modes will be locked, unlocked, or facility code.
   j) Input power will be 12VDC +/- 10% @ 400mA with an operating range of 10VDC to 16VDC.

d. Alarm Input Module (AIM)
1) The AIM will monitor all system alarm inputs. The following requirements will apply:
   a) The AIM will provide up to 16 supervised alarm inputs to monitor and report fault conditions (open, short, ground, or circuit fault) alarm conditions, power faults, and tampers. Upon alarm activation, the associated alarm condition will be reported to the IC and subsequently to the system alarm monitoring workstation.
   b) Light emitting diodes (LED) will indicate the status of the sixteen (16) alarm zones, cabinet tamper, and power fault.
c) The Alarm Input Modules will operate independently and in conjunction with the Relay Output Modules (ROM), which will send an output signal to a corresponding output device upon alarm activation. Upon alarm activation, the AIM will activate any or all alarm outputs within the ROM. The OM will provide Sixteen (16) Form C outputs rated at 5A @ 30VDC. Upon receipt of an alarm input from the AIM, the ROM will transmit an activating signal to a corresponding output device.
d) Up to 32 AIMs will be connected to an available IC via RS-485 cabling.
e) Diagnostic light emitting diodes (LED) will indicate IC communication, input zone scanning, and AIM heartbeat.
f) The AIM will contain the following features:
g) Alarm contact status scanning at up to 180 times per second for each zone.
h) Eight- (8) configuration DIP-switches to assign unit addresses and communications speed.
   (1) A low power CMOS microprocessor.
   (2) Filtered data for noise rejection to prevent false alarms.
   (3) Two form C, 2A @ 28V dc contacts for load switching.
   (4) Two dedicated inputs for tamper and power status.
   (5) Individual shunt times (ADA requirement).
   (6) Input power will be 12VDC +/- 10% @ 350mA with an operating range of 10VDC to 16VDC.

2) All Inputs will be completely configurable by the system operator for inclusion in logical device definition. Inputs will not be defaulted by the System for unalterable designation. For example, input #1 defaults as door contact for door #1, input #2 defaults as Request to Exit device for door #1, etc. Systems that do not allow for user definition of all input points will be unacceptable.

I. Relay Output Module (ROM)
1) The ROM will incorporate 16 output relays that are capable of controlling a corresponding output device upon any input activation or on command from the system. Relay Outputs will be capable of responding to:
   a) Input alarms from within the same IC.
   b) Commands from a system operator.
   c) Time zone control commands for automatic operation.
   d) Output relays will be capable of:
      (1) Pulsing for a predetermined duration that will be programmable for each relay individually.
(2) Following any input point an AIM attached to the same IC (ON with alarm, OFF when clear, or as required).
(3) Responding on command from the system operator to pulse, command on, command off, or reset to normal state.
(4) Each ROM will provide sixteen (16) Form C relays rated at 2A @ 28VDC. The ROM will control the relays via digital communication. Upon receipt of input from the AIM or command from the system operator, the AIM will transmit an activating signal to the corresponding relay.
(5) Input power will be 12VDC +/- 10% @ 400mA with an operating range of 10VDC to 16VDC.

e) All Outputs will be completely configurable by the system operator for inclusion in logical device definition. Outputs will not be defaulted by the System for unalterable designation.

B. Access Cards
1. Proximity type card activated by the card reader.
2. Card will be 3.375 inches by 2.125 inches and 0.036 inch thick
3. Use 125 kilohertz frequency for activation and communications.

C. Card Readers
1. Proximity Card Readers will be provided at the specified locations.
2. These will be installed at the height shown on the drawings.
3. The cabling to the readers will be shielded and grounded as per the manufacturer's instructions. Care should be taken to avoid errant contact between the shield and doorframe.
4. Transmits a 125 kilohertz frequency for card activation and communications.
5. The reader style and finish will be selected from the manufacturer's product list as shown on the installation documents.
a. Power: The reader will be powered by 5VDC or by the controller's internal 12VDC regulated power supply.
b. Mounting: The reader will be capable of being mounted against metal door or window frames.
c. Range: The reader will be capable of reading cards at a range of five to eight inches.

D. Door Alarm Contact Switches
1. Be DPDT hermetically-sealed, magnetic reed-switch.
2. Be Reed-potted in contact housing, with a polyurethane-base compound.
3. Have Snap-lock housing into a 15/16” diameter hole (flush mount).
4. Be molded of a flame-retardant ABS plastic.
5. Have Color to match the doorframe in which it is mounted.

E. Passive Infrared Exit Detector

1. Uses passive infrared technology to detect persons passing through its field of view.
2. Have an adjustable detection pattern large enough to assure activation of the door contact switch shunt circuitry at the intelligent door controller prior to door opening (yet adequately limited in size to keep erroneous activation to a minimum).
3. Be provided with two (2) form “C” contacts.
4. Be wall and ceiling mountable.
5. Have internal, vertical point ability.
6. Have up to sixty- (60-) second adjustable latch time.
7. Capable of selectable relay trigger mode.
8. Have selectable fail safe / fail secure mode.
9. Have color selected by College Representative.
10. Capable of 12 or 24 AC or DC Operation.
11. Be UL-Listed.

F. System Power:

1. The System will operate using standard 120VAC, 50/60-Hz power.
2. The connection to the main building power supply will be performed in accordance with the general terms and conditions of this contract.
3. This will include connection to and provision of Uninterrupted Power Systems (UPS) when specified.

G. Enclosure Power:

1. A separate power supply enclosure will be directly connected to a convenient diConnect panel.
2. The diConnect breaker will be clearly marked.
   a. An inline transformer, rated at 12VDC, 4A continuous power will provide power.
   b. The power enclosure will be provided with LED indicators showing normal operating conditions, loss of AC power-standby battery supplying power, loss of AC power, discharged or no standby battery, and no DC output.
   c. The enclosure will include a 12VDC, 7-amp hour battery, securely fastened to the enclosure to prevent the accidental removal of the battery.
   d. It will be capable of providing backup from 1 to 5 hours depending on module configuration.

4.04 VIDEO SURVEILLANCE

A. IP Network based enterprise class Digital Video Surveillance System will allow the display of live, record and playback of digital video streams from multiple video surveillance IP cameras, simultaneously, on the System’s operator console and/or on other display and control platforms including clients, virtual matrix
display, notebook computer, and Cell phone.

B. The system will be 100% non-proprietary and have an open architecture technology.

C. Video from any of the cameras will be available for viewing after entering proper password credentials anywhere on the College’s network (wired and wireless) using a web browser or a software application.

D. There will be universal camera and hardware support.
   1. A variety of IP type cameras will be supported by the system.
   2. Hardware from various manufacturers will be supported.

E. Video Management Software general system and system administration requirements:
   1. Run as a Windows Service without the user interface (web based) or as a Windows Application with the user interface (software application).
   2. Support F1 (Help) function for getting content-sensitive build-in help system.
   3. Provide an option to use Active Directory services to authenticate remote users.
   4. Communicate and receive video image streams from IP addressable Cameras using IP protocol.
   5. Support traditional analog cameras via video server adapters using IP protocol.
   6. Control PTZ cameras using IP protocol.
   7. Support DNS entries.
   8. Support IP cameras and encoders using MJPEG, MPEG4, Wavelet and H263 compression simultaneously.
   9. Have the ability to view, record, playback and archive video from cameras located at remote locations over the IP network. (Multi-location recordings).
   10. Simultaneously record, playback and display live video and audio (Triplex).
   11. Allow time synchronized multiple cameras view/playback with motion detection information.
   12. Allow the access to view/playback multiple cameras from other workstation on the network.
   13. Have the ability to record and store images at rates between 1 frame per hour to 30 frames per second on a per camera basis.
   14. Have the ability to store the recorded images on the System’s local hard drive or on a Network Attached Storage (NAS), or on attached storage (USB, Firewire, and SCSI) as required.
   15. Support unlimited number of cameras per server, from which maximum 64 can be viewed or recorded by operators at the same time.
   16. Be scalable to support any number of cameras with multiple consoles.
   17. Have automatic (maintenance free) daily archiving capabilities of recorded video with automatic archive recycling.
   18. Have the capability to allow for automatic off-premises video archiving on
19. Be capable of performing multiple archiving per day.
20. Have video search capabilities to find video images by Time, Date and Activity/Alarm.
21. Provide a twenty-four (24) hours scheduler to activate and deactivate the following features on a per camera basis:
   a. to bring cameras on/off line
   b. to sound audible alarm on motion detection in camera’s field of view
   c. to send e-mail/text pager/SMS notification on motion detection events with/without video image attachment
   d. to start/stop and change patrolling sequence for PTZ cameras
22. Provide red Motion Detection indicator light for each camera, to indicate if motion detected by camera when operator left the station and comes back.
23. Provide yellow Event indicator light for each camera, to indicate if event happened on the camera.
24. Will have an advanced motion detection capabilities.
25. The operator will have the ability to use one, several or any non-conflicting combinations of the following functions, on a per camera basis:
   a. automatically freeze the live video of a camera with no motion in its field of view
   b. stop recording camera images with no motion in it field of view
   c. start recording images up to 999 seconds before a motion is detected in the cameras field of view and continue recording for up to 999 seconds after the motion stopped in the cameras field of view
   d. adjustments of motion level sensitivity from 0 – 10,000 units in 1 unit increments
   e. adjustments of low light noise levels from 0 – 256 units in 1 unit increments to avoid false motion detection
   f. up to 1024 inclusion / exclusion motion detection zones per camera.
   g. Change recorded frame rate when motion is detected
26. Have the option to start recording on an event setup by the operator/administrator.
27. Be able to speedup the recording FPS on motion detection or on event detected.
28. Have the ability to adjust image resolution to QCIF 160x120, CIF 320x240, VGA (4CIF) 640x480 and up to 2,048 x 1,536 lines
29. Be capable of adjusting the compression level of the video image data size, to save on storage size, when needed.
30. PTZ camera capabilities:
   a. provide the operator with up to 25 presets position per PTZ camera and the ability to quickly cause the camera to move to a preset location upon operator demand
   b. be able to move a PTZ camera to any of the preset positions upon detecting motion at another camera
   c. have the ability to cause the PTZ camera to go to any of the preset positions on input contact closure/open (such as door sensor, alarm panel input etc.)
d. have the ability to provide PTZ camera patrolling feature between preset positions

e. be able to program unlimited number of patrolling sequences, each with unlimited number of presets list selected from 50 possible presets

f. capable of controlling the patrolling sequences using a 24/7 scheduler.

g. be able to control PTZ movement speed during patrolling for selected supported PTZ cameras

h. be able to resume patrolling an operator manual control times out without moving the PTZ

i. have the option not to record while moving between presets and will stay in a preset position if motion was detected in the camera field of view at that preset position, and will continue patrolling once motion stopped

31. Be able to support closure and open of remote relay output at the IP cameras and/or video server adapters.

32. Be able to detect close/open relay input from the camera’s location and trigger alarm/event on the System.

33. Have the ability to detect door contacts or PIR motion detector input and cause a PTZ camera to move and zoom into the door and record the activity, to increase protection of sensitive areas.

34. Be able to perform “go to preset” on event even during patrolling sequence.

35. Be able to define “ASCII Generated Events”.

36. Provide tamper-proof log file on users’ activity in the system using encryption and integrity check.

F. Video Management Software main console / operator station:

1. The System will include an operator station/console for local video surveillance management.

2. Be able support at least 2 display screen per operator console, one for live view of all cameras, simultaneously (monitoring screen), and the other display for playback, search, video clips productions, evidence printout and more (viewer screen). Playback and searching will not interfere or eliminate the continuous and simultaneous view of the live streaming videos.

3. Display all active cameras on the monitoring screen, in a 2x2 and up to 8x8 matrix.

4. Allow the operator to zoom, pan and tilt any PTZ camera by using the System’s mouse.

5. Allow the operator to zoom, pan and tilt selected supported PTZ camera with USB Joystick device.

6. Have the ability on selected supported to manual zoom, manual iris and brightness control on the joystick panel with quick return to auto mode.

7. Have the ability to start/stop recording and speed up frame rate.

8. Allow the display of each live camera on a larger then original image size screen. (Large view).


10. Have a Viewer application with the ability to show multiple selected
cameras at the same time with full synchronization between the images.

11. Playback viewer screen will provide the operator with ability to skip forward and backward the video on a frame-by-frame basis, event-by-event basis and provide 3 levels of fast-forward / backward playback.

12. Playback viewer screen will provide the operator with graphical motion level bar for quick identification of motion events and the ability to access the event by mouse click and drag in to graph area, on a per camera basis. (Search by activity)

13. Playback Viewer screen will provide the operator with search tools to find video sequence by entering date and time of event. (Search by date/time)

14. Playback Viewer screen will provide the operator with search tools to find video according to motion at certain area of the image (Smart Search). Operator will be able to define area of interest in 32x32 grid, define motion sensitivity and frequency.

15. Provide additional viewer(s) with the ability to view live or archive information from selected cameras.

16. Have the ability to send video streams to additional monitors on the local IP network, as needed - requires NetMatrixMonitor (one license will be included).

17. Provide the following general alarm and notification via sound, system message and e-mail/pager: General System alarms, low video storage space, camera disconnect.

18. Provide digital zoom into pre-recorded video with image improvement option.

19. Have an export tool to copy video and audio to a CD or DVD incorporating a “watermarking” technique that will determine if any of the pictures in the video have been modified in any way.

20. Have export tool of recorded video and audio using the system database format with date and time stamp.

21. Have the ability to encrypt the database exported file with user key of minimum 64 bits.

22. Have the ability to compress the database exported file.

23. Have export tool of recorded video into JPEG or AVI formats and the ability to e-mail and store these files.

24. Be able to create AVI for selection of multiple cameras.

25. Have printer tool to allow the operator to print video image and add operator name and comments as well as print a system timestamp of the event.

G. CCTV system Remote Access via Web server using Internet Explorer:

1. Provide web server service to allow authorized users to view live video, playback of recorded video and search the archive to view video using their Internet Explorer web browser from any PC on the Intranet or Internet, if authorized.

2. The web browser functionality will include:
   a. provide username and password for access control into the System
   b. define remote user profile and user rights in relation to viewing certain cameras and the use of PTZ and Output relays
   c. navigate to cameras and rooms using and integrated premises
d. view any MJPEG camera on the System, with live video
e. control all 25 PTZ Presets per camera for fast and accurate remote positioning control
f. access any recorded video of the current day and the archive for past days, search by time/date or activity/alarm and playback the video as a stream, frame by frame or jump to motion detected sequences
g. provide thumbnail images for each new event for easy search
h. create an AVI file video and audio clips of desire sequences with time stamp for local storage and the ability to e-mail it
i. allow printout of still image with operator comments and timestamp.
j. provide a view of live video from 4 cameras, simultaneously
k. activate remote system relay outputs to control external systems as light, sounds and wipers

H. Remote Access via Client Software:

1. Provide Image server service to allow authorized users to view live video, playback of recorded video and search the archive to view video using installed client software based on .net technology.
2. The client will be downloaded from the recording server.
3. Will include unlimited number of viewer/playback clients able to:
   a. provide username and password for access control into the System
   b. define remote user profile and user rights in relation to viewing certain cameras and the use of any function within the client
   c. define user profile and views as an individual user or as shared features between multiple users
   d. monitor up to 64 live cameras on the same screen or on multiple screens
   e. each camera window can be defined as a live/playback camera, map, fixed image, hotspot and incoming video alarm window.
   f. select cameras using “drag and drop” from the camera list
   g. select cameras using integrated premises map
   h. each camera will go to full screen by double click on the image
   i. cameras recorded on multiple recorders throughout the network can be viewed on the same screen
   j. create unlimited number of views and screen grids, arranged into groups
   k. flip between Views using Keyboard or mouse
   l. use clickable maps to call different camera views
   m. full PTZ control includes sending the camera to any of the 25 presets
   n. control PTZ camera with Point and Click
   o. control selected supported PTZ camera with USB Joystick
   p. control PTZ camera setting with buttons on the USB joystick
   q. controlled functions includes manual focus, iris control and gain control.
   r. control PTZ camera using Keyboard functions including pan, tilt
and zoom
s. synchronized playback of cameras with forward and backward commands, fast forward, fast backward, forward playback, reverse playback, playback speed control and frame-by-frame commands
t. control playback by keyboard inc. frame by frame, next or previous sequence.
u. digital PTZ on live and recorded image
v. find recording using Go-To time and date
w. find recording using Alarm / Event list
x. find recording using “Smart Search”
y. automatic archive search for activity in a designated area of the image
z. preview clip of any alarm/event sequence of a pop up window
aa. export an AVI file to the client desktop
bb. print still picture from any camera with operator comments
cc. change screen grid and cameras locations selected from pull down menu on the fly
dd. arrange grid and cameras location in logical hierarchy of Groups and Views
ee. set up camera layout on the grid using drag and drop from the available cameras list.
ff. able to import alarm list for specific camera and view alarm preview clip
gg. supports audio feed with the video supports

I. Virtual Matrix for Automatic Event-Driven Push Live Video to a control room or desktop monitor.

J. Integration with Virtual Matrix for complete control room video wall display platform - NetSwitcher.

1. Ability to call and camera to any monitor using clickable maps
2. Ability to select the monitor using point and click on the controller touch screen
3. Ability to switch between live and playback on the fly.
4. Ability to push live video on event to any of the monitors.

K. Cameras:

1. Standard resolution fixed cameras will be predominately used on each of the campuses.
a. outdoor application
b. resolution 752x480 pixels (4 CIF minimum)
c. progressive scan imager
d. veri-focal lens 4mm to 10mm
e. .4 lux minimum illumination
f. multi-zone motion detection
g. wide dynamic range up to 100db.
h. digital PTZ
i. light enhancement technology for improved color night viewing
j. heater/blower (requires voltage adapter and extra 2 conductor
2. 1.3 megapixel cameras will be used in areas requiring a higher resolution as noted on the drawings.
   a. outdoor application
   b. resolution 1.3 megapixels (1280x1024 pixels)
   c. progressive scan imager
   d. veri-focal lens 4mm to 10mm
   e. .2 lux minimum illumination
   f. multi-zone motion detection
   g. digital PTZ
   h. 15 images per second at max resolution
   i. light enhancement technology for improved color night viewing
   j. heater/blower (requires voltage adapter and extra 2 conductor cable)
   k. IP addressable
   l. RJ 45 connector
   m. IEEE 802.3af PoE
   n. clear polycarbonate (hi-impact vandal resistant) dome housing.
   o. pendent adapter and wall mount.

3. A panoramic megapixel camera will be used to cover the center quad area of three campuses as noted on the drawings.
   a. outdoor application.
   b. 180 degree or 360 degree (Watsonville HS) view for maximum coverage
   c. four 2 mega-pixel cameras in a single dome housing
   d. resolution 2 megapixels per camera (4 cameras)
   e. progressive scan imager
   f. fixed Lens
   g. 1 lux minimum illumination
   h. heater/blower (requires voltage adapter and extra 2 conductor cable)
   i. IP addressable
   j. RJ45 connector
   k. IEEE 802.3af PoE
   l. clear polycarbonate (hi-impact vandal resistant) dome housing.
   m. pendent adapter and wall mount.

L. Server:

1. Each campus will have a server located in the MDF or where designated by the College; coordinate with College for location.

2. As a minimum the server will be a two (2) rack unit (2u), rack mounted server configured as follows:
   a. Intel® Dual Core Xeon® 5130 (2.0Ghz 1333Mhz FSB) Processor
b. 2 GB Memory  
c. Smart Array P800 Hard Drive Controller  
d. 2 - 146Gb Hot Plug 2.5 SAS 10,000 rpm Hard Drives  
e. 2 Embedded NC373i Multifunction Gigabit Network Adapters  
f. 1u Server 700w Hot Plug Power Supply  
g. Redundant fans  
h. CD-RW/DVD RW Drive  
i. DVD-Dual Layer Burner  
j. 3 year manufacturer’s warranty- 3 years parts and labor, next business day  
k. Microsoft Windows Server 2003  

M. Additional Archival Storage  
1. Archival storage will be for approximately 30 days at each server location.  

4.05 COURTESY CALL STATIONS  

A. Wall Mounted Call Station with Blue Light  
1. The Call Station will be a single enclosure containing all lights, a button, a PS, and unit electronics in a wall-mounted enclosure. The Call Station will have the following features:  
a. Single unit assembly that mounts to wall.  
b. Alarm outputs.  
c. Emergency call button “CALL FOR HELP”.  
d. Courtesy Call button “INFO”  
e. Twenty four- (24-) hour visibility constant illumination, blue light.  
f. Blue strobe upon unit activation.  
g. Comply with ADA requirements, CBC mounting height section 1118B.  
h. Hands-free communication after initial activation.  
i. Be vandal resistant.  
j. Voice identification.  
k. “COURTESY” will be displayed on the sides.  

B. Free Standing Call Station with Blue Light  
1. The Call Station will be a single free-standing pole enclosure containing all lights, a button, a PS, and unit electronics. The Call Station will have the following features:  
a. Nine (9) feet tall, eight (80) inches round  
b. Mounts to concrete base.  
c. Alarm outputs.  
d. Emergency call button “CALL FOR HELP”.  
e. Courtesy Call button “INFO”  
f. Twenty four- (24-) hour visibility constant illumination, blue light.  
g. Blue strobe upon unit activation.  
h. Comply with ADA requirements, CBC mounting height section 1118B.  
i. Hands-free communication after initial activation.
j. Be vandal resistant.
k. Voice identification.
l. “COURTESY” will be displayed on the sides.

4.06 CONDUIT, CABLES, AND INSTALLATION MATERIALS

A. Conduit and Related Materials

1. Non-metallic conduit will be rigid PVC electrical conduit extended to Schedule 40 or 80 dimensions of Type II meeting Nema standards, reference Nema RN-1. Grade 1 high impact, polyvinyl chloride, sweeps, couplings, reducers and terminating fillings will be listed under the UL re-examination service, and will bear UL Label and manufacturer's listed marking. Couplings, elbows, bends, connectors, and other fittings for PVC will be of appropriate manufacture for PVC use. Reference Nema TC-3.

2. Electrical Metallic Tubing (EMT), for indoor use only, will be steel tubing, will meet standards under ANSI C80.3. EMT will be zinc coated with protective coating inside that enhances cable pulling efforts. Couplings, elbows, bends, connectors, and other fittings for EMT will be gland compression type and of appropriate manufacture for EMT use.

3. Metallic conduit and tubing will be galvanized standard weight meeting standards under ANSI C80.1. Rigid conduit will be manufactured under supervision of UL, Factory Inspection and Label Service Program. Each 10'0" length of Conduit and tubing will bear UL Label, manufacturers name, and listed marking. Couplings, elbows, bends, connectors, and other fittings for metallic conduit will be of appropriate manufacture for metallic conduit use.

4. Use of Intermediate Metal Conduit, IMC, for external exposed use is permitted.

5. Junction and Pull Boxes
   a. Junction and pull boxes, in addition to those indicated, will only be used where absolutely necessary with the specific direction of the College’s representative in each case.
   b. Concealed interior boxes will be constructed of blue or galvanized steel with ample laps, spot welded, and will be rigid under torsional and deflecting forces. Boxes will have auxiliary angle iron framing where necessary to ensure rigidity. Covers will be fastened to the box with a sufficient number of brass machine screws to ensure continuous contact all around. Flush type boxes will be drilled and tapped for cover screws at the site if the boxes are not installed plumb. All surfaces of pull and junction boxes and covers will be given one coat of metal primer, and one coat or aluminum paint.
   c. All junction and pull boxes will be rigidly fastened to the structure and will not depend on the conduits for support.

B. PENETRATIONS IN FIRE RATED STRUCTURES/ASSEMBLIES

1. Existing assemblies and structures to be encountered typically will include minimum 1-hour fire rated walls and ceilings and 2-hour fire rated shaft
2. All firewalls penetrated by structured cabling will be sealed by use of a non-permanent fire blanket or other method in compliance with the current edition of National Fire Protection Association (NFPA) and the National Electric Code (NEC) or other prevailing code.

3. The contractor must not use concrete or other non-removable substance for fire stopping on cable trays, wire-ways, or conduits.

4. Contractors who use this fire method will be required to replace all cables affected and provide the original specified access to each affected area.

5. Fire stop system must be UL classified for through-penetration applications of metallic conduits.

6. Provide 3M caulk and fire barriers for making fire rated seals around all penetrations as required per code.

C. PULL STRINGS

1. 1/4” polyetherine or nylon cord will be installed in each flew and existing conduit. Underground service conduits will also include pull strings.

D. HOOKS AND SUSPENSION SYSTEMS

1. J-hooks, strut or trapeze systems, etc. will be acquired as appropriate for the construction effort and will be compliant with all building codes and standards of construction for the intended purpose.

E. BACKBOARDS

1. All backboards will be ¾” AC fire treated, Class 1, UL stamped plywood.

2. If painted, will be painted with fire-resistant paint in a color complementing location.

3. Backboards will be attached to walls with mechanical fasteners such as drilled concrete type wedge anchors, screws, or bolts. Toggle bolts are not permitted.

4. Backboards will be sized as follows:
   a. When backboard is within secure room, etc. the backboard will typically be 8’ x 4’ x ¾” when wall space permits and sized accordingly when wall space is a limiting factor, but must be sufficient to house all necessary components to be placed on backboard.
   b. When located in exposed area within office, classroom, etc. the backboard will be cut to match the dimensions of the locking cabinet that will be mounted on the backboard, and painted with fire-resistant paint to the color of the wall when possible.

F. EQUIPMENT CABINETS/RACKS

1. Wall mount swing rack – 24” and 48”
   a. 19” rack mount frame, 18 – 20” deep with height sized from 24” and 48” selection below.
   b. Left or right side hinging.
   c. Universal hole spacing per EIA 310-D.
d. 19” style rails tapped #12-24 holes 5/8”, 5/8”, ½” EIA standard hole pattern, front and back.

e. Support up to 100lbs.

f. The equipment rack will be properly grounded per code and manufacturers recommendations.

g. Preferred product:
      a) 24” - HPWWMR24
      b) 48” - HPWWMR48

2. Wall mount locking cabinet – 24” and 48”
a. 19” rack mount frame, sizing 26” deep with height selected from 24” and 48” selection below.

b. Left or right side hinging of door.

c. Fully adjustable rails, front to back.

d. Universal hole spacing per EIA 310-D.

e. 19” style rails tapped #12-24, front and back.

f. 2 sets of universal mounting rails with #12-24 tapped holes 5/8”, 5/8”, ½” EIA standard hole pattern.

g. Support up to 150lbs.

h. Acrylic window door.

i. The equipment rack will be properly grounded per code and manufacturers recommendations.

j. Preferred product:

   a) 24” - MCC24WMC19, approx. 24”h x 21”w x 26”d
   b) 48” - MCC48WMC19, approx. 48”h x 21”w x 26”d

3. Wall mount, low profile equipment cabinet, secure.
a. Overall approximate dimensions of 32” high x 24” wide, wall mounted cabinet for 19” rack mounting of 2 or 4 hubs/switches, space for 48/96 port patch panels.

b. 2 sets of universal mounting rails with #12-24 tapped holes 5/8”, 5/8”, ½” EIA standard hole pattern.

c. The equipment rack will be properly grounded per code and manufacturer’s recommendations.

d. Reference product:

   a) Two (2) rack-mount units, Model RE2
   b) Four (4) rack-mount units, Model RE4

G. WIRE AND CABLE

1. The following are acceptable products.
a. Data horizontal wiring
   1) Category 5e, 100 Ω active 4-pair, 24AWG, UTP workstation cabling as defined in EIA/TIA TSB-36 for Category 5e cable.

   2) Reference products:
      a) Certified Category 5e cable from AT&T, Belden, or Com/Scope, General Cable, Berk-Tek, Mohawk..

2. Inter-building fiber optic cabling
a. Six (6), twelve (12), or twenty-four (24) multi-mode fibers, ISO
(International Standards Organization) and FDDI (Fiber Distributed Data Interface) standard, 62.5/125 micron core diameter fiber optic cable.

b. The number of fibers installed will be per documentation.

c. All multi-mode fibers will be fitted with AT&T SC type connectors of appropriate manufacture.

d. Reference products:
   1) Cabling will be AT&T, Beldon, Berk-Tek, Commscope, General Cable, Mohawk, Optical Cable Corporation, or Seicor duct-rated cabling for exterior installation.
   2) Base-line example - AT&T multi-mode fiber cable product, 3DAX-012-HXM.

3. Pre-manufactured Category 5e data patch/station cords

a. Must meet or exceed TIA/EIA 568-A Category 5e cable.

b. Round in shape and consisting of eight insulated 24 AWG, stranded copper conductors, arranged in four color-coded twisted-pairs within a flame-retardant jacket.

c. Equipped with modular 8-position (RJ45 style) plugs on both ends, wired straight-through with 568B, AT&T style, wiring methodology.

d. Modular plugs must exceed FCC CFR 47 part 68 subpart F and IEC 60603-7 specifications, and have 50 microinches minimum of gold plating over nickel contacts.

e. Resistant to corrosion from humidity, extreme temperatures, and airborne contaminants.

f. Must utilize cable that exhibit power sum NEXT performance.

g. Must maintain shield continuity through the modular plug shield and not via the contacts when screened (ScTP) cords are used.

h. Gray or black in color.

i. Without hoods.

j. Electrical Specifications:
   1) DC resistance per lead: 9.38 Ω / 100 m maximum.
   2) Input impedance without averaging: 100 Ω ± 15% from 1 to 100 MHz.
   3) 100% transmission tested with laboratory grade network analyzers for proper performance up to 100 MHz. Vendor will guarantee cords are compatible with category 5e links.
   4) UL VERIFIED (or equivalent) for TIA/EIA category 5e electrical performance.
   5) UL LISTED 1863.

k. Reference products:
   1) Manufactured by an ISO 9001 and 14001 Certified Manufacturer.
   2) Certified Category 5e cable from AT&T, Belden, Hubbell, Mohawk, or Com/Scope.

H. Pre-manufactured fiber optic patch cables

1. Standard lengths of 1, 3, and 5 meters must be available, custom lengths will also be available, and will meet or exceed standards as defined in ANSI/TIA/EIA-568-A and ISO/IEC 11801.

2. Duplex fiber cable must be 62.5/125, OFNR riser grade, and will meet the
requirements of UL 1666.
3. Attenuation will not exceed 3.5 dB/km @ 850 nm wavelength or 1.0 dB/km @ 1300 nm.
4. Cable jacket color must be orange for 62.5/125.
5. The connectors will be SC and perform in accordance with TIA/EIA-568-A; the SC connectors must include a ceramic ferrule.
6. Terminated SC connectors must exhibit a maximum insertion loss of 0.65 dB with an average of 0.40 dB when tested at either 850 nm or 1300 nm wavelengths for both 50/125 and 62.5/125 μm.
7. A minimum return loss of 20 dB (25 dB typical) at both 850 nm & 1300 nm.
8. Must be manufactured by an ISO 9001 and 14001 Certified Manufacturer.
9. UL 1666 approved.

I. DATA OUTLETS, single gang

1. Single-gang plate must provide for six receptacles.
2. Reference product
   b. Plates - FPL16 series with color to match design specification.

J. DATA TERMINATIONS

1. Black anodized aluminum, in 24-port or 48-port configurations.
2. Must accommodate at least 24 ports for each rack mount space (1rms = 44.5 mm [1.75 in.]).
3. Must have circuit boards tested in both directions as required by ANSI/TIA/EIA-568-A and ISO/IEC 11801.
4. Must have category 5e jacks available in universal T568A/T568B wiring and T568A or T568B wiring schemes, with 110-style termination.
5. Must allow for a minimum of 200 re-terminations without signal degradation below standards compliance limit.
6. Must have modular ports compliant with FCC CFR 47 part 68 subpart F and IEC 60603-7 with 50 microinches of gold plating over nickel contacts.
7. Must allow the use of a 4 or 5-pair 110-style impact termination tool.
8. Must be fully enclosed front and rear for physical protection of printed circuit board.
9. Must have cable tie eyelets and a rear cable management bar for strain relief.
10. Must have port identification numbers on both the front and rear of the panel.
11. Must have an optional adhesive circuit identification and color coding designation strips provided with the panel.
12. Must provide self adhesive, clear label holders and white designation labels with the panel, with optional color labels available.
13. Must accept 110 style patch plugs as a means of termination.
14. Must be available in a 24-port version that exceeds the transfer impedance requirements of ISO/IEC 11801. This panel must accept two types of cable preparation for termination.
15. 110 patch panels will contain no less than 24 ports and no more than 48 ports and sized for the application; panels should be acquired in the
smallest rack unit (ru) size possible.

16. Electrical Specifications:
   a. ANSI/TIA/EIA-568-A and ISO/IEC 11801 proposed category 5e compliant.
   b. Patch Panels will be insulation displacement EIA/TIA-T568B wiring Category 5e compliant.

17. Reference product:
   a. Must be made by an ISO 9001 and 14001 Certified Manufacturer
   b. AT&T 110 modular rack mount jack panels available with 24 or 48 jacks.

K. Fiber Optic Interconnect Centers, Panels and Trays.

1. All interconnect centers, panels and trays (units) will provide cross-connect, inter-connect, splicing capabilities and contain cable management for supporting and routing the fiber cables/jumpers.

2. Wall Mount
   a. Must have a low profile, compact design, able to accommodate up to 12- or 24- port for the Mini version and 48- or 96 -port for the standard version enclosure.
   b. Must accommodate SC, ST, MT-RJ, and LC adapters.
   c. Must accommodate hybrid adapter plates for ST-to-SC or SC-to-ST connections.
   d. Must be modular in design with management clips that provide two independent levels of slack storage to comply with fiber bend radius and the recommended slack storage length.
   e. Must have an administrative labeling system available on a hinged door capable of latching or locking for protection.
   f. Must have six, eight and twelve port fiber adapter plates that allow for color coding on the 6 and 8 port versions.
   g. Must have fiber adapter plates with snap-in installation and one-finger removal.
   h. Must have an optional version with an integrated jumper guard that has a hinged and lockable door separate from the main cable management section.
   i. Must have anchor points, and a strain relief thumbscrew for the fiber cable entry to the unit.
   j. Must accommodate stackable splice trays that manage up to a total of 48 splices.
   k. Must be available in black or white and constructed of 18 gauge steel.
   l. Must be UL listed 1863.
   m. Must be made by an ISO 9001 and 14001 Certified Manufacturer.

3. Rack-Mounted, High Density Fiber Interconnect Center
   a. Must be available in white or black, and made of 12 gauge aluminum alloy.
   b. Must be available in up to 24, 32, 48, and 72 port versions with ST and SC fiber adapters preloaded into adapter plates or 48, 64, 96 and 144 port versions using quad SC, MT-RJ, and LC fiber adapters preloaded into adapter plates.
c. Must have preloaded adapter plates with ST and SC fiber adapters in 6 port version, ST and SC in 8 port version, as well as a 12 port version for the SC MT-RJ, LC adapters.
d. Must have blank adapter plates for future growth of the fiber infrastructure.
e. Must have fiber managers to effectively store fiber cable slack and comply with fiber bend radius requirements.
f. Must have six and eight port fiber adapter plates which allow for color coding connectors.
g. Must have fiber adapter plates with snap-in installation and one-finger removal in both flat and angled versions.
h. Must have lockable front and rear transparent doors that have spring release hinges for removal.
i. Must accommodate stackable splice trays, each tray manages a total of 24 splices.
j. Must have an adapter plate mounting bracket which slides out to the front and to the rear of the unit for increased access.
k. Must have cable access points for fiber jumpers entering and exiting the unit with rotating grommets to facilitate cable loading and to minimize microbending stress.
l. Must have anchor points for fiber cable(s) entering the unit.
m. Must have labeling which meets or exceed ANSI/TIA/EIA-606 requirements and also be laser printable.
n. Must be able to mount 19-inch.
o. Must be UL listed 1863 and cUL C22.2 approved.
p. Must be made by an ISO 9001 and 14001 Certified Manufacturer.

4. Rack-Mounted, Low Profile Fiber Connect Panel
a. Must not be bigger then one rack mount space and accommodate up to 36 ports for SC, MT-RJ, or LC adapter plates or 18 ports for ST or FC adapters plates.
b. Must have preloaded adapter plates with ST and SC fiber adapters in 6 and 8 port version, as well as a 12 port version for the SC, MT-RJ and LC adapters.
c. Must have blank adapter plates for future growth of the fiber infrastructure.
d. Must have six and eight port fiber adapter plates which allow for color coding connectors.
e. Must have fiber adapter plates with snap-in installation and one-finger removal.
f. Must accommodate hybrid adapter plates for ST-to-SC or SC-to-ST connections.
g. Must be modular in design with internal fiber managers that provide slack storage to comply with fiber bend radius and the recommended slack storage length.
h. Must have a snap-on front shield to be used as a labeling surface and to protect jumpers. This shield can also relocate to another position during termination to maintain circuit identification.
i. Must accommodates a splice tray for mechanical or fusion splices.
j. Must be available with a drawer mechanism which allows the panel to slide forward or to the rear and has a defeatable latches.
to allow removal from the rack or cabinet.

k. Must be made by an ISO 9001 and 14001 Certified Manufacturer.

5. Rack-Mounted Fiber Tray
   a. 18 gauge steel with a black finish.
   b. Available in 16-, 24-, 28-, 32- and 48-port configurations, and be able to double that port count utilizing 4-port adapters.
   c. Accommodate SC, ST, MT-RJ and LC adapters.
   d. Accommodate hybrid adapter bezels for ST-to-SC or SC-to-ST connections.
   e. Have changeable ports which are removed from the front of the unit to allow custom configuration or modification.
   f. Have silk screened port identification numbers provided on both the front and rear of the panel.
   g. Include fiber managers that manage slack storage so as to comply with fiber bend radius requirements and slack storage length recommendations.
   h. Accommodate stackable splice trays which manage up to 24 splices per tray.
   i. Have a smoked polycarbonate cover with quarter turn screws for easy access.
   j. Must not exceed a 254 mm (10 in) depth for mounting in standard cabinets and enclosures.
   k. Must be equipped with strain relief lugs for the fiber cable entering the unit from the side or back.
   l. Must be made by an ISO 9001 and 14001 Certified Manufacturer.

L. Surface Mounted Raceway
   1. Plastic raceway providing for horizontal and vertical cable paths, transitions, and connections where recessed and other hidden pathways are not available.
   2. Product line must allow for multi-channel and support for electrical as needed.
   3. Raceway must be capable of secure attachment with means other than glue or sticky-backing.
   4. Component, connections, transitions to match design specification.
   5. Color to complement existing environment.
   6. Reference Products:
      a. Wiremold 5xxx Series and miscellaneous single channel products.
      b. Hubbell MediaTrak products.
PART 5 INSTALLATION STANDARDS

5.01 CABLING INSTALLATION

A. General

1. All cable runs in ceiling areas must be assessed by the College as to whether or not the space is a plenum air return space, which will dictate the use of a listed plenum type or PVC type cable as required in the materials specification.
2. The cables will be routed to their respective Security Panel, Main Distribution Frame (MDF) or Intermediate Distribution Frame (IDF), and Node Termination Point (NDP) utilizing the shortest path possible.
3. Station cable (UTP) or (STP) runs are not to exceed 90 meters.
4. Conduit fill capacity will be at 40% unless governing standard or College permission provides for different capacity.

B. Fiber Optic Cabling (Data only)

1. Fiber optic cabling will be utilized in the following situations:
   a. When the distance between any two points exceeds 275 feet and cannot or should not be reconciled with switching electronics.
   b. Building to building transitions where environmental conditions will subject to feed to excessive moisture or mud.
   c. Transitions that are subjected to electrical interference.
   d. Service feeds from 3 feet to 1,000 feet where performance issues require fiber optic links.
   e. Special circumstances where required by electronics, vendor, or application.
2. Multi-mode fiber, ISO (International Standards Organization) and FDDI (Fiber Distributed Data Interface) standard, 62.5/125 micron core diameter; multi-mode fiber optic cable will be installed and terminated on SC type connectors in the LIU.
3. Connectors: AT&T SC type connectors, or approved equivalent, will be installed.
4. All fiber optic cable terminations in a distribution box will have at least 36 inches of slack from end kit to the SC connector when in the same fiber distribution box (FDB). All fiber optic cable terminations that pass into a second FDB will have at least 48 inches of slack. Enough cable play must be left so that the fiber distribution box drawer / cable tray can be opened for servicing without damaging any of the cables.
5. There will be a minimum of fifteen (15) feet of cable slack in each fiber optic cable left in each IDF area, mounted in a circular fashion.
6. There will be a minimum of thirty (30) feet of cable slack in each fiber optic cable left in the MDF area, mounted in a circular fashion.
7. Manufacturer’s bending radius specification will be maintained.

C. Cabling Run Paths
1. All cable will be hidden as much as possible
2. Splices are not permitted, except when authorized in advance and in writing by the College, and only under circumstances where it is in the College’s best interest to allow the splice to occur.

D. Cable Pulling

1. Cable pulling will be handled with care as to not damage the cable itself or the facilities it is pulled into and by.
2. A pulling methodology; including fish tape, cable, or rope that potentially can damage the raceway will not be used.
3. Restrictive use of pull compound or lubricant.
   a. Will only be used when necessary and only with written permission from the College.
   b. Pulling compound must be a water base pulling lubricant that will not deteriorate cable or conduit.
4. Cables WILL NOT be:
   a. Pulled across sharp edges.
   b. Forced or jammed between metal parts, assemblies, etc.
   c. Allowed to rest on any ceiling tile or suspension system unless specifically authorized by the College.
   d. Pulled across access doors and pull box covers. Access to all equipment and systems must be maintained.
5. Cables WILL be:
   a. Pulled free of sharp bends or kinks.
   b. Kept 30-inches away from any heat source; i.e., steam valves, etc.
   c. Where high voltage is present in interstitial space, kept away from the conduits as far as possible.

E. Cable Routing

1. Cables will be run in corridors wherever possible in order to avoid furniture and work areas so that access to the cables is unencumbered.
2. The cables are to be as accessible as possible, placed below all other items in the ceiling, including ducts and supports.
3. The cables will be placed at a minimum of 18 inches above the ceiling to allow enough space for the lighting fixtures.
4. Low-voltage cabling must be separated by a minimum of six (6) feet from main power panels, electrical switch components and starter motors.
5. Power delivery systems greater than 220 volts must not run parallel to low-voltage cabling. Parallel runs of greater than twenty (20) feet require a minimum separation distance of three (3) feet, or 18” inches if cables are contained in a metallic conduit that is grounded.
6. Multiple conduit runs of 110 volts power distribution must not run parallel to low-voltage cabling. Parallel runs of greater than twenty (20) feet require a minimum separation distance of 18”.
7. There must be an 18-inch separation between the cables and the fluorescent light fixtures.
8. In cases where an 18-inch separation between fluorescent light fixtures and the cables cannot be achieved, then RF suppression will be provided by the College on all fluorescent light ballasts.
a. Contractor will notify the College in the event this requirement cannot be met.

9. Cable connected to electrified door hardware will be kept away from other data cables due to the possibility of interfering with data as a result of the potential current/voltage spikes on the electrified door hardware wire.

F. Cable Securing and Identification

1. Transposing or changing color coding of wires is acceptable only with College’s approval.
2. Cable bundles in raceways, in suspension systems, or on wallboards must be tie wrapped every 4 feet.
3. All cabling must be installed with proper stress relief and tied down.
4. Station cables must be strapped with tie straps every 4 feet. Strapping to any other wires (e.g., lighting, ceiling grid, etc.) is not permitted.
5. Fiber Optic cable/cables must be identified with a tag as to the system and date, every 50 feet when installed in open trays or suspension systems in ceilings.

G. Cable Termination

1. All cable terminations will be accomplished according to the appropriate industry standards for the cable and terminal involved, subject to the requirements as presented in Section 3.0 – DESIGN STANDARDS.
2. Sufficient cable loops will be provided at all terminal points for stress relief, potential cable re-termination, and cable relocation.
3. All wire-to-wire and wire to EOL resistor will be soldered and taped.
4. Use of splice caps, or crimp-on splice devices will not be acceptable.

H. Cable Labeling

1. All labeling will be performed in accordance with EIA/TIA 568, 569, and 606 standards. A marked drawing of each building’s/floor horizontal cable identification numbers will be attached to the wall in each IDF room. Also, a marked drawing of all fiber optic cable identification numbers will be attached to the wall in the MDF area.
2. Each drawing will indicate the cable identification of every single cable that is installed by the contractor.
3. Additionally, two (2) copies of drawings of each building’s cable ids and the location of all fibers will also be provided to the College.
4. All face plates and patch panels will be labeled with a clear plastic typewritten label. A 3M or Panduit self-laminating write-on label (Panduit part number PSCD-3) or equivalent) will be used. All information written on cable labels will be done with the use of a permanent marker (Sanford ultra fine point pen) and be legible. Each label will be placed 6 inches from the end of each cable.

I. Cable Testing.

1. All field tests will be performed as specified in this document.
2. All cabling and terminations will be tested according to appropriate
industry standards and generally accepted industry practices with the most severe and strenuous used as the base-line level of acceptance.

3. All cables will be subjected to continuity testing with cables properly identified and labeled at each end.

4. After conduits, conductors, and enclosures have been installed, but prior to any equipment being interconnected, all wiring and cabling will be checked to insure there are no foreign grounds, opens, or shorts on any conductors or shields.

5. Category 5e cable
   a. A Category 5e TIA/EIA TSB-67 Level II compliant cable tester will be used to test all intra-building Category 5e cables for certification of operation at 100Mbps. These tests will include: wire-map, length, delay, NEXT, attenuation, ACR, impedance, loop resistance and capacitance information.
   b. All cables certification reports will include: circuit id, PASS result, cable tester and injection type, date test was performed, NVP for cable, location information, office end or patch panel end, name of tester and signature.
   c. The NEXT and ACR will be measured at each end of the cable (at the wall outlet and at the patch panel). If however, the cable injector used can simultaneously perform measurements at both ends of an installed link, the test need only be performed once. The cable certification report must show the ability of the injector to perform both tests simultaneously.
   d. All cable testers will be calibrated at the beginning of each day.
   e. Specifications to be made available by addendum and will appear as an appendix. Contractor will confer with College at point in time well before cable testing begins.

6. Fiber optic, multi-mode
   a. Specifications to be made available by addendum and will appear as an appendix. Contractor will confer with College at point in time well before cable testing begins.

7. The NVP calibration will be performed using a known quantity of the cable (100’ or more) on a daily basis.

5.02 SURFACE MOUNTED RACEWAY

A. Single or multi-compartment surface mounted raceway, depending on requirement, will be utilized to mount all workstation outlets not recessed into wall. (Typically mount at 24” at top of raceway, but locate as application demands.)

B. All appropriate surface raceway fittings, connectors, junction boxes, duplex cover plates, and the like will be utilized per manufacturer's recommendations; copies of which must be made available to the College.

C. 6” base section will be utilized for stronger holding power.

D. Outlet locations are approximate when specified in project documentation. Final placement will be modified wherever possible to accommodate code and the
installation of the raceway. Final raceway placement will be approved by College prior to installation. It is the contractor’s responsibility to notify the College of any conflicts, or potential conflicts prior to installation to avoid delays and/or installation problems.

E. Provide surface raceway as indicated in project documentation.

F. Provide toggle bolts or red head anchors to support surface raceway, plastic anchors are not acceptable. Raceway must have adhesive backing plus 3 screws for every 6’ section. Screw raceway in middle of each section and within 3” from each end.

G. End caps in areas where transitions through walls are occurring will allow for up to four (4) ¾” sleeves, and two (2) 1” sleeves.

H. End cap bushings will be installed at end of each raceway run.

5.03 CONDUIT INSTALLATION

A. General

1. Conduit will carry product listing and be appropriately classified for installation and use
2. Continuous system of rigid or PVC conduit, outlet boxes, junction boxes, fittings, racks, and cabinets for all cabling backbone systems is required, except as expressly allowed by College.
3. Conduit will be concealed unless otherwise permitted by College. Conduits exposed to view, except those in attic spaces and under buildings, will be installed parallel or at right angles to structural members, walls, or lines of building. Conduits will be routed in such a manner to provide clear access openings.
4. Conduit runs will contain no more than four (4) quarter turns (90° bends) between pull boxes, backboards, etc.

B. Conduit Usage

1. Outside exposed:
   a. Intermediate Metal Conduit, IMC, will be used for outside conduit running along breezeways, on roofs, as risers, etc.
   b. Conduit mounted on roofs will be subject to specific mounting requirements in order to maintain roofing warranties. All installation will require coordination with College’s Maintenance and Operations.
   c. Conduit will be painted to match the specific area the pipe travels in.

2. Within buildings:
   a. EMT may be used in lieu of rigid metallic conduit where permitted by code.
   b. Within buildings, rigid metal conduit will be discouraged if high performance raceway, i.e. Wiremold 5400, can be used effectively instead.
3. Underground:
   a. Schedule 40 PVC will be used for underground.
   b. Schedule 80 will be used for transitions to the surface.
   c. Appropriate sealants and gluing will be used.

4. Transitions:
   a. Outdoor connections between IMC conduit runs and pull boxes, etc. will be made with IMC transitions bent according to bending radius rules.
   b. Flexible seal tight tubing will be used for short, 5’ or less, between buildings for cabling that is not considered to be high volume backbone.

C. Trenching

1. Trenches will be designed to minimize intrusion into areas that have high aesthetic value, i.e. grass areas, expensive grade paving, public presentation areas.
2. Trenches will be dug at a minimum of 24” and proceed as straight as possible.
3. Sand bed of 2” will be placed over rocky or other abrasive areas.
4. Warning tape of appropriate designation will be laid on layer of earth that rises 6” to 10” above level of top of uppermost pipe in trench.
5. Once the trench is dug and ready for pipe the trench must be inspected by College staff.
6. Once the pipe has been placed in trench with risers to surface, College staff must inspect the pipe installation before the pipe is covered with dirt.
7. If the above are not adhered to it will be necessary to remove the dirt and expose the pipe and trench for inspection at contractor’s expense in time and materials.

D. Bends or offsets

1. Will not be permitted unless absolutely necessary.
2. It will be the responsibility of Contractor to install conduit with a minimum of bends, and in such a manner as to conform to structure and meet all applicable codes.
3. All required bends and offsets will be made with standard tools and equipment designed specifically for the purpose, or factory made bends or elbows complying with requirements for radius of bends specified as follows:
   a. 1 ½” conduit 18” minimum radius
   b. 2” conduit 24” minimum radius
   c. 3” conduit 36” minimum radius
   d. 4” conduit 48” minimum radius
4. Conduit bends not specified above must have a radius that is not less than 10 times the diameter of conduit.

E. Additional boxes.

1. Install additional boxes beyond original plan where needed to prevent damage to cables and wires during pulling operations; Contractor is
expected to anticipate need.

2. If Contractor specified the quantity, type, size, and location of boxes then cost of additional boxes will be borne by Contractor with no cost to the College.

3. Size boxes per NEC.

4. Running threads will not be permitted; provide approved conduit unions where union joints are necessary.

5. Conduit will be kept at least 6” away from coverings on hot water pipes and 18” away from flues and breachings.

6. All conduits are to be sealed with standard non-hardening sealing compound to prevent the entrance of debris, moisture, and gases during installation and to meet fire resistance requirements.

7. All conduits are to remain sealed until wiring is installed.

F. Joints

1. Joints will not be permitted in conduits installed in concrete.

2. Joints in wet locations, exposed to weather or underground will be made liquid tight.

3. Conduit threads will be filled with approved electrical pipe joint compound before screwing into couplings and threaded fittings.

G. Terminations

1. Where conduits are terminated in groups at backboards, equipment racks, cabinets, etc. provide rigid material frames or appropriate spacers to hold conduit in secure position and to preserve alignment.

2. Conduits terminating at equipment racks and cabinets will enter cabinets in the following approved locations only:
   a. Conduits entering top and bottom of cabinets will be aligned in a single row, centered 2” from rear of cabinet or rack.
   b. Conduits entering back of cabinet will be aligned in a single row centered 2” from top of cabinet.
   c. Conduits will not be spaced closer than 3” on centers.

H. Pipe Straps/Hangers/Racks

1. Conduit in ceiling spaces, in stud walls, and under floors will be supported with uni-strut and will hold conduit tight at point of support against ceiling and floor joists, rafters, wall studs, or 2” x 4” headers fitted between joists or wall studs.

2. Conduits installed on existing exposed structural members will be fastened with factory-made conduit straps or clamps, which will hold conduit tight against supporting member at point of support.

I. Bushings

1. Will be threaded insulating type for all sizes of rigid steel conduit.

2. Setscrew bushings are not acceptable and will not be used or permitted.

J. Knockouts
1. Remove only those knockouts as required for conduit installation.
2. Plug any unused openings as follows:
   a. Use threaded plus for cast metal boxes.
   b. Snap-in metal covers for sheet metal boxes.
   c. Apply sealant for weatherproofing.

K. Penetrations

1. Penetrations in beams and roofs are not permitted.
2. Penetrations in concrete walls to be core-drilled only.
3. Sleeves of appropriate type for conduit used must be provided and installed where conduits pierce concrete walls.
4. Sleeves must have ½” clearance around conduits.
   a. Sleeves will not extend beyond thickness of exposed surfaces of concrete.
   b. Sleeves will be securely fastened to forms and adjacent construction.
5. Where conduit passes through walls below grade, caulk with approved sealant and backer materials between conduit and sleeve to obtain a watertight joint.
6. Upon penetrating building from the outside, 18” x 24” x 6” J-boxes will be installed on both the interior and exterior sides of the wall to allow for adequate sweeps.
   a. Exterior boxes to be waterproof.

5.04 ENCLOSURES, J-BOXES, AND CABINETS

A. Security System/Fire Alarm/CCTV/Access electronics and all boxes in the area of the Security Panels will be housed within metal enclosures with keyed alike locking doors (located in secure spaces and contain TSs to indicate when the key-operated doors are opened)

B. Separate UL-listed enclosure(s) for isolation relays, fuses for the electronically-controlled locking hardware, and miscellaneous devices will be provided and sized appropriately for the number of devices to be housed (if used)

C. J- and pull-boxes will be sized as required

D. J-Boxes will be secured with tamper-resistant screws or locks on an enclosure with a lockable door

E. If the J-Box is located less than 10 feet above the finished floor, an additional pair of wire and a TS will be required

F. The tamper will be connected to the nearest available input point

G. Processors, power supplies, and other related equipment will be mounted at the Security Panel location on a fire-rated plywood backboard

H. Manufacturer-recommended mounting hardware will be used for securing ceiling mounted devices
I. Seismic bracing on appropriate equipment will be installed

J. Security fasteners will be provided on all J-Box, pull-box, and low-voltage electrical gutter cover-plates

K. J-Boxes will be clearly marked for easy identification

L. The front of the Security System panels will be labeled with the name of the installing Contractor, company address, service phone number, and the date that warranty expires

M. A copy of panel wiring and associated as built drawings will be located in a pouch attached to the inside door of an Access Door Controller

5.05 PANEL WIRING AND TERMINATION:

A. Conductors will be carefully formed and neatly harnessed with tie-wraps spaced 1 inch - 2 inch apart so that each drops off directly opposite its terminal

B. Conductors will be run parallel to the insides of the enclosure

C. Small wire duct (if space permits) may be used in lieu of tie-wrapping the conductors as long as there are no exposed multiple conductors greater than 4 inch in length

D. Wire and cable will be routed away from heat producing components such as resistors, regulators, etc.

E. Conductors will be labeled, within 4 inch from each end, with permanent marking labels and will be easily readable

F. A termination will be made so that there is no bare conductor at the terminal

G. Conductor insulation will bear against the terminal or connector shoulder

H. Spade lugs will be used on the end of conductors attaching to screw-type terminals as much as practical with the wire securely fastened

I. Enclosure barrier-strips or connector terminals will be numbered and coded. Controls, function switches, etc., will be clearly labeled on all equipment panels

5.06 GROUNDING:

A. Appropriate grounding will be provided as called out in the Specifications and Drawings or specified by the manufacturer

B. Earth ground will be connected to ground rod or approved cold water pipe

C. Electrical or telephone ground connections will not be used as earth grounds

D. Connections to mounting posts or building structural steel will not be used as earth grounds
5.07 DOORS AND DOOR HARDWARE:
A. Nothing will be done to modify a fire-rated door or frame that would void the fire rating, otherwise the door may need to be re-certified

5.08 POWER TO SECURITY EQUIPMENT AND POWER SUPPLIES:
A. All equipment from 120VAC circuits dedicated for security use will be powered except as noted. All panel circuit breakers will be marked Security Equipment - Do Not Operate

B. Any panic hardware that requires a separate 120VAC power booster will have that power booster located within 150 feet of the door hardware; distance is dependent on wire gage as follows:
   1. 2C #14 AWG stranded for exit devices up to 75 feet from power booster
   2. 2C #12 AWG stranded for exit devices up to 150 feet from power booster

C. Plug-in transformers will be located at the security control panels in a lockable, tampered, ventilated electrical enclosure

D. A single duplex power receptacle with power hard-wired to the receptacle will be provided within the enclosure (a power-strip may be used within the electrical enclosure)

E. Transformers will be clearly labeled to identify purpose and use of each