DESIGN STANDARD FOR TELECOMMUNICATIONS

Purpose:

The purpose of this document is to standardize the basic elements of the telecommunications systems design process. The design standard has the purpose of creating a consistent application of telecommunications systems design throughout the Solano Community College (SCC) District, therefore achieving a standard of quality for maintenance and reliability throughout all renovation and new building projects. This standard serves as a supporting document part of the overall Solano Community College Technology Plan (2013-2015). Deviations from this standard shall be approved by SCC.

Telecommunications Systems-Related Support Staff and Committees:

Chief Technology Officer
Director, Technology Services & Support
Desktop Services
Network Services
The Strategic Technology Advisory Committee (STAC)

Design Standard:

I. TELECOM IDF/MDF ROOMS

A. Minimum size of the IDF is to be 8’ x 9’.

B. Minimum size of the MDF is to be 10’ x 13’ and shall not be co-located with electrical equipment due to EMI-mechanical noise transmitted from the electrical equipment.

C. IDF should have a hard ceiling for security purposes.

D. IDF/MDF rooms should not have any water sprinklers in the room.

E. Room must be well lit. Lighting fixtures shall be coordinated with any horizontal cable tray or other ceiling mounted equipment.

F. No equipment other than that related to the voice/data network should be located in the IDF’s/MDF’s. This includes but not limited to FACP, lighting control equipment, electrical panels, EMS, etc.

G. Regular 110v receptacles should be located at standard locations around the room.
H. Some form of standalone air conditioning must be provided to adequately cool the space when fully equipped. Cooling capacity shall be calculated taking into account all equipment planned for the room. Rooms should not be on building Air system.

I. There should be 3’ of clear space on all 4 sides of the 2’ x 3.25’ cabinet. If necessary for placement of an additional cabinet or future placement of an additional cabinet this requirement can be modified to 3’ of clear space in the front, rear and one side of the cabinet.

J. Lock to IDF/MDF must be uniquely keyed and only Technology Services & Support staff is to be issued keys. In cases where an IDF is shared with Maintenance & Operation (M&O), only essential M&O staff is to have keys to the IDF/MDF (i.e. Engineers, Director, and Assistant Director). Before issuing a key to anyone for any IDF/MDF the Director of Technology Services & Support must be consulted.

K. Where possible, doors to the IDF/MDF should not have windows or signage other than room numbers (for security purposes). If IDF/MDF doors must have windows, windows are to be blacked out.

L. A phone is to be located on one wall of the IDF/MDF room, typically on the door wall.

II. CABINETS

A. Refer to the document SCC – TSS Telecommunications Cabling Materials List for standard cabinet models and accessories (fan kit).

B. Secure cabinet(s) to floor utilizing CPI brackets and drop-in anchors.

C. Secure top of cabinet(s) utilizing appropriate size ladder rack attached to cabinet with CPI elevation kits.

D. Install CPI vertical wire managers and fan-kits to cabinet. Fans shall be connected to power and operational.

E. Install cabinet provided vertical wire management @ rear of cabinet.

F. Install square punched rails in cabinet; contractor to provide necessary cage nuts and mounting screws for all equipment being installed in rack.

G. Install hardware in cabinet based on 1. = top U holes:

1. Fiber LIU (with single-mode fiber terminated first left to right and then followed by MM). LIU shall be installed in the top 1U of the cabinet
2. Wire management shall be installed on the sides of the patch panels as well as between each Data/Voice patch panel.

3. Data patch panel(s) shall be KRONE CAT 6 and 568B compliant.

4. Copper cable (CAT3) terminated on patch panel. All data patch panels shall be terminated first, and then the CAT 3 cable shall be terminated on a voice patch panel at the end of the data patch panel sequence. There shall be one pair per port (termination on the White/Blue pair for voice) with the Violet/Slate pair un-terminated and left as a spare.

5. District supplied network switches

6. District supplied UPS

7. District supplied PDU (extra outlets for equipment)

H. Two electrical outlets (30amp w/L5-R30 receptacles) to be installed @ top of rack height inside cabinet.

I. Customer provided UPS power cord will be run from UPS on floor of cabinet through rear vertical wire manager to electrical outlet.

III. BACKBOARD LAY-OUT

A. Refer to the document SCC – TSS Telecommunications Cabling Materials List for standard cabling materials.

B. Backboard: 4’ X 8’ X 3/4” plywood should be installed on only one wall (to be determined by cabinet position)

C. Backboard shall be installed starting 4” above the finished floor, shall be fire-rated plywood painted white. Fire rated sticker shall not be painted over.

D. Copper feed cable is to be terminated in appropriate sized protected terminal (50pr, 100pr etc.). Terminal is to be grounded to bus bar.

E. CAT3 copper cable to be terminated on “out” of protected terminal to patch panel in cabinet. (routed overhead on ladder rack)

IV. CABLING & CABLE ROUTING

A. Refer to the document SCC – TSS Telecommunications Cabling Materials List for standard cabling materials.
B. All drop cables routed into MDF/IDF to be installed through appropriate sized sleeves with bushings.

C. All drop cables to be “split out” by number (ie; 1-12, 13-24) and brought into cabinet on opposing sides of patch panel.

D. All cables will be tested for compliance (using MicroTek or similar device) with results provided to district in printed and in an electronic form acceptable to the district.

E. All ladder rack to be grounded to provided bus bar.

F. Labeling standard is Room#-drop (i.e. 128-10) number starting in left corner of room and moving clockwise around room. Drops number are sequential from room to room (i.e. 128-20, 129-21, etc.).

G. All cables to be terminated 568B.

H. All phone connectivity is to be VOIP with all cables to be ADC blue CAT6.

I. Customer/Architect to determine PVC vs. plenum rated cable.

J. ADC faceplate and jack insert color is typically Ivory.

K. Cable numbering to be determined by sequence: floor, closet #, drop number. Two drop locations to be labeled 1/2 and three plus drop locations to be labeled 1-3. Example: 1st floor closet # 1 would read: 1.1.1/2 or 1.1.1-3.

L. All fiber required to be extended shall match existing hybrid fiber count.

M. All fiber will be tested using OTDR with results provided to district in printed and in an electronic form acceptable to the district.

N. Extended fiber shall be fusion spliced in approved fiber splice case.

O. Single mode patch cords are to be installed from fiber LIU to fire panel. Alarm vendor will plug in @ panel.

P. Copper cable required to be extended can “splice thru” on A110 blocks.

Q. All cabling should be routed according to industry standards and supported in cable hangers or cable trays.
R. Cable hangers will not be attached to ceiling tie wires. The first choice by cabling vendor will be to install their own wires or wall mount hangers. Where this is not possible due to existing conditions, there may be existing wires that are unattached to the grid or utilized for other mechanical support that can be utilized.

S. Industry standards apply to fire stop installation and will be dictated by field conditions.

T. Phones are to be co-located with data and terminated on patch panel in cabinet.

U. Need data runs for HVAC (copper) and fire alarms (fiber). A cat 6 drop must be placed near the HVAC controller. A fiber patch cable must be run in conduit from the FACP location to the IDF.

V. Standard is Cat6 cabling.

W. Cabinet as well as station patch cords are to be provided by contractor in lengths and quantities as specified by customer (usually the number of ports terminated for cabinet quantity–3’& 7’ lengths).

X. Standard drop count for an employee work location is 3 drops. Standard drop count for a student station is 1 drop plus 1 printer drop for every 20 computers.

Y. Standard materials are to be used as listed on the Solano Community College - Technology Services & Support Telecommunications Cabling Materials List.

Z. All building projects must include above ceiling cabling for installation of PoE wireless access points.

AA. Electronic and printed forms of as built drawings must be provided to IT.

BB. All newly installed cabling must be tested and performance test results shall be submitted to SCC IT.

V. WIRELESS NETWORK

A. All building projects must include installation of wireless access points to cover the interior of the building (location diagram will be supplied by district).

B. All interior wireless access points are Power over Ethernet (PoE) and therefore DO NOT require a power receptacle to be placed near the access point device.

C. All exterior wireless access points have an external antenna and the device MAY REQUIRE a power receptacle to be located in close proximity to the device. Coordinate requirements with SCC IT.
D. Wireless access points require a Cat6 cable terminated with an RJ45 connector in a biscuit box to be located per the district supplied drawings and routed to the IDF/MDF. Every effort should be made to keep the wireless access point cables to be terminated in a group on the patch panel and clearly identified. Cabling and termination is vendor supplied (i.e. patch panels, biscuit box, etc.).

E. Access points are to be mounted per manufacturer supplied instructions and are generally surface mounted on the ceiling at district specified locations. Actual placement can vary slightly depending on conditions at the specified locations.

F. All cabling to access points are to be tested per industry standards.

G. All wireless access points are district supplied/contractor installed.

VI. PHONES

A. All phones are to be VoIP phones except where analog lines are necessary (i.e. emergency phones, fax lines, etc.).

B. District standard VoIP phones are CISCO brand.

C. All VoIP phones plug into CISCO PoE (Power over Ethernet) switches.

D. Lines for emergency equipment (emergency phones, fire alarms, security alarms, etc.) are to be 1MB’s provided by the district’s Telco carrier and NOT part of the district phone system.

E. Each building is to have wall mounted courtesy/emergency phones in each hallway.

VII. ACCESS TO TELECOM SPACES

A. Contractors shall contact SCC IT for proper badging and access to telecom spaces. Request for access shall be submitted in writing and follow the District’s guidelines and procedures.
Typical IDF Room Layout

Approved Manufacturers:

Equipment Racks and Cabinets:

1. Middle Atlantic Products
2. CPI – Chatsworth Products
3. Panduit

Wireless Access Points:

1. Refer to SCC IT for list of approved manufacturers

Copper Patch Panels:

1. Panduit
2. Siemen
Fiber Patch Panels:

1. Panduit
2. Siemens

Category Cable / Patch Cords:

1. General Cable
2. Mohawk
3. Berk-Tek

Fiber Cable / Patch Chords:

1. General Cable
2. Mohawk
3. Berk-Tek

Wire Managers:

1. Middle Atlantic Products
2. CPI – Chatsworth Products
3. Panduit

Ladder Rack / Cable Tray:

2. Refer to SCC IT for list of approved manufacturers

Substitutes Allowed:

All substitutions must be approved by SCC IT. Requests for substitutions must be submitted in writing prior to design, purchase, and installation.
Associated Design Standards and Construction Specifications

Standards
EIA/TIA-568 Commercial Building Telecommunications Wiring Standard
TIA-569 Telecommunications Pathways and Spaces
TIA-607 Generic Telecommunications Bonding and Grounding for Customer Premises
TIA-942 Telecommunications Infrastructure Standard for Data Centers
ANSI/NECA/BICSO-56-2006 Standard for Installing Commercial Building Telecommunications Cabling
ANSI/NECA/BISCI-607 Telecommunications Bonding and grounding Planning and Installation Methods for Commercial Buildings
ANSI/BICSI-002 Data Center Design Standard and Recommended Practices

Specifications
270500 COMMON WORK RESULTS FOR COMMUNICATIONS
271100 COMMUNICATIONS EQUIPMENT ROOM FITTINGS
271300 COMMUNICATIONS BACKBONE CABLING
271500 COMMUNICATIONS HORIZONTAL CABLING

End of Document
DESIGN STANDARD FOR ELECTRONIC SAFETY AND SECURITY

Purpose

The purpose of this document is to standardize the basic elements of the Electronic Safety and Security systems design process. The Design Standard has the purpose of creating a consistent application of Electronic Safety and Security systems design throughout the Solano Community College (SCC) District, therefore achieving a standard of quality for maintenance and reliability throughout all renovation and new building projects. Deviations from this standard shall be approved by SCC.

Table of Contents

Abbreviations .............................................................................................................................................................................. Error! Bookmark not defined.

Design Standard—Security Systems Ownership.................................................................................................................... 4

SCC Executive Leadership .............................................................................................................................................................. 4

SCC IT ........................................................................................................................................................................................................ 4

Security Systems Contractor/Integrator ........................................................................................................................................ 5

SCC Engineering & Plant Ops ..................................................................................................................................................... 5

Design Standard—Electronic Access Control System (EACS) ................................................................................................. 5

System Criteria ........................................................................................................................................................................ 5

Access Control Application Criteria ....................................................................................................................................... 6

Design Standard—Video Management System (VMS) ................................................................................................................ 7

System Criteria ........................................................................................................................................................................ 7

Camera Application Criteria .................................................................................................................................................... 8

Design Standard—Intrusion Detection System (IDS) ................................................................................................................ 9

System Criteria ........................................................................................................................................................................ 9

Intrusion Detection System Application Criteria .................................................................................................................. 10


Automated Notification Message Broadcasting Service ........................................................................................................ 12
Indoor Public Address .......................................................................................................................... 12
Outdoor Public Address ....................................................................................................................... 12
Outdoor “Blue Tower” Emergency Telephones .................................................................................. 12
Design Standard— Crime Prevention through Environmental Design (CPTED) .................................... 13
Approved Manufacturers ..................................................................................................................... 13
Substitutes Allowed .............................................................................................................................. 14
Associated Design Standards and Construction Specifications .......................................................... 14
Addendum ‘A’ ......................................................................................................................................... 14
Abbreviations

- SSA – Security Sensitive Areas
- P&P’s – Policies & Procedures
- LED – Light Emitting Diode (type of lighting with preferable heat generation and energy consumption characteristics over traditional incandescent luminaires)
- PV – Photovoltaic (solar panels)
- EMNS – Emergency Mass Notification Systems
- PA – Public Address (overhead speakers)
- AV – Audiovisual
- LAN – Local Area Network (IP network based Ethernet data network)
- IDS – Intrusion Detection System (burglar alarm)
- PIN code – Personal Identification Number (numerical code entered on arming station keypad to arm or disarm an Intrusion Detection System)
- ARM – arming station keypad used to arm or disarm an Intrusion Detection System
- MD – Motion Detector (intrusion detection sensor)
- EACS – Electronic Access Control System
- ACP – Access Control Panel
- CCTV – Closed Circuit Television (older, traditional term for analog video surveillance system)
- VMS – Video Management System (newer term for IP network based video surveillance system)
- NVR – Network Video Recorder
- PTZ – Pan Tilt Zoom video surveillance camera (remotely operable in lieu of fixed)
Design Standard – Security Systems Ownership

An effective security program requires comprehensive administrative and operational planning, direction, oversight, and control. With regard to security electronics systems – including electronic access control, video surveillance, intrusion detection, and emergency communications – the “ownership” of the security systems by various associated parties must be clarified, codified in policy, assigned, and accepted.

There are 4 primary parties that must be assigned and must accept responsibility and accountability for various functions of service and maintenance as well as daily operation of the security systems. Importantly, such accountability cannot be reasonably and successfully assigned unless the associated party is also granted the authority, staffing, and funding to carry out the responsibility.

SCC Executive Leadership

1. Provides the authority, authorization, oversight, and funding for systems deployment and use.
2. Issues Policies & Procedures.
3. Determines the appropriate end-users of the system from both law enforcement professional security personnel and departmental staff personnel.
4. Coordinates the functional and operational system requirements between Academic and departmental representatives.

SCC IT

1. Provides network connectivity and support.
2. May provide computing hardware such as servers and computer workstations for use by the Security Systems Contractor/Integrator.
3. Ensures appropriate network security, firewalls, and encryption issues are addressed and documented.
4. Maintains scheduled maintenance of security systems software versions, licenses, and firmware (when such activities are not outsourced to the Security Systems Contractor/Integrator).
5. Maintains scheduled maintenance of security systems hardware operating system, antivirus software, utilities, and system activity logs.
6. Coordinates authorized login UserID and passwords with the network domain identity structure.
Security Systems Contractor/Integrator

1. Provides, installs, programs, configures, and tests the security systems hardware and software.
2. Warrants the installation for one year from date of project substantial completion.
3. May be engaged under contract to provide extended warranty including work order service and preventative maintenance beyond the one year project warranty.
4. This role may be filled by one or more contractors.

SCC Engineering & Plant Ops

1. Provides, installs, programs, configures, and tests the security systems hardware and software as needed above and beyond the scope of the Security Systems Contractor/Integrator and when the Security Systems Contractor/Integrator is no longer under contract.
2. Provides, installs, and maintains door/frame assemblies and electrified locking door hardware.
3. Maintains traditional physical keying system with documented issuance and retrieval audit logs.
4. Provides the lead role in coordinating the efforts of the Security Systems Contractor/Integrator with SCC Executive Leadership, IT, project design team, and the work of other trades and contractors.

Design Standard—Electronic Access Control System (EACS)

Refer to Addendum ‘A’ at the end of this document for the Electronic Access Control System Standard.

Design standards ensure that Electronic Access Control System installations, retrofits, replacements, and upgrades maintain system consistency and compatibility — regardless of project timing or funding source. These EACS Standards also support a single system database to avoid redundancy, duplication, and error, facilitate system administrator training and back-up, facilitate service and maintenance, and act as a record document that can be periodically updated to reflect new developments and requirements.

System Criteria

1. SCC will deploy a single standardized, centralized, and compatible Electronic Access Control System at all campuses
2. System will primarily consist of card readers, electrified locking door hardware, alarm contacts, request-to-exit (REX) sensors and access control server hardware/software
3. System will secondarily consist of wireless locksets which communicate with the centralized access control server hardware/software

4. Electrified locking door hardware should be hardwired for low-voltage power

5. Electronically access controlled doors shall be capable of being locked and unlocked in an automated manner based on schedules in the EACS software

6. All access control points shall communicate with the centralized access control server hardware/software and shall not be ‘stand-alone’; all electronic access control devices shall provide wireless or hardwired communication to the standardized centralized access control system software platform

7. Access to access control system cardholder and access rights database shall be through the use of authorized client software only; authorized persons shall be issued a secure unique login and password

8. Authorized client access to system shall be customized based on the user’s role: for example: full-privilege rights system administrator versus limited-privilege rights end-user with control over a limited subsection of the cardholder and access rights database

The Electronic Access Control System shall:

1. Be purpose-built for access control functionality
2. Support wireless and hardwired access control locking door hardware
3. Support integration with software for the maintenance of the traditional “hard key” Keying System
4. Supported by numerous local competitive contractors
5. Should not require recurring licensing fees
6. Support the use of technology-based access credentials whether photo ID badge or key ring fob or other form factors; credentials shall be programmed for customizable specific access rights per individuals

**Access Control Application Criteria**

Electronic access control with electrified locking door hardware shall be designed, provided, and installed on the following doors in the following order of priority:

1. Building exterior entry/exit doors: these are entryways which provide the primary access to the building; these are the doors which are intended to be capable of being locked/unlocked on a
scheduled basis. The number of designated entry/exit doors should be limited in number to funnel traffic to these doors, the doors must have door closers and no door prop mechanisms, and must unlock without unlatching when “open” according to the pre-programmed schedule.

2. Building interior additional doors shall be installed with electronic access control devices pending confirmation by Solano Community College on a project-specific case-by-case basis in coordination with the project teams:
   a. MDF/IDF data network equipment closets
   b. Computer labs
   c. Smart classrooms
   d. Lost & Found or other asset storage areas
   e. Security Sensitive Areas

The following doors have access control considerations other than electronic access control with electrified locking door hardware:

1. Emergency exit only doors shall have no exterior trim (no exterior lockset knobs/lever handles or key cylinders) unless required by SCC or the Authority Having Jurisdiction. These doors shall be used for exiting only and should not be used as entry doors into the building.
   a. They may be locally alarmed with door prop alarms to indicate that the door has been left open, these locations shall be determined on a project-specific case by case basis.
   b. Where door prop alarms are used they should be hardwired for low-voltage power and supported by appropriate signage.

**Design Standard—Video Management System (VMS)**

**System Criteria**

1. SCC will deploy a single standardized, centralized, and compatible video surveillance system at all campuses
2. System will consist of cameras, cabling, Power-Over-Ethernet (PoE) data network switches, and Network Video Recorder (NVR) hardware/software
3. System shall be IP network (Ethernet) based; no analog cameras or other system components shall be specified, provided, or installed
4. Cameras shall primarily be homerun hardwired with cabling; cabling shall be Ethernet cabling of a Category confirmed by SCC; this CAT cable shall be Power-Over-Ethernet (PoE) to provide signal and low-voltage power in a single homerun cable.

5. Cameras shall secondarily be on wireless point-to-point connections only where the costs of providing a hardwired connection is greater than the costs of providing a wireless link (e.g. parking lots).

6. Access to live or recorded video shall be through the use of authorized client software only; authorized persons shall be issued a secure unique login and password.

7. Authorized client access to system shall be customized based on the user’s role: for example: full-privilege rights system administrator versus limited-privilege rights “view/search only” end-user.

8. System will primarily consist of fixed cameras; Pan-Tilt-Zoom (PTZ) remotely operable cameras shall be specified, provided, or installed only on a project-specific case-by-case basis. PTZ cameras may be a required programmatic system component to be specified at the discretion of SCC, such as Cafeteria and Quad areas.

9. Where a camera is installed near an electronic access control door the door should be in the field of view of the installed camera.

10. 30 days recording minimum.

**Camera Application Criteria**

Video surveillance cameras shall be designed, provided, and installed at the following areas in the following order of priority; camera placements shall be coordinated with projects that are pending in the SCC Master Plan so that projects are not installing cameras that will subsequently be removed:

1. Primary campus vehicular entry/exit lanes; though these cameras are not intended to be software-based “License Plate Recognition (LPR)” cameras they should be mounted low with IR illuminators in order to provide views of vehicles and license plates. These installations typically leverage an available local power source such as a light-pole and may utilize underground conduit runs or wireless point-to-point to send the video signal to a building where the recording equipment is installed.

2. Parking lots general views as confirmed in design projects by SCC; coordinated with obstructions, trees/landscaping, and PV panels; may include bus stop and drop-off/pick-up curbs.

3. Building primary pedestrian entry/exit doors associated with electronic access controlled doors.

4. Building secondary pedestrian entry/exit and emergency exit only doors.
5. Building second floors points of vertical transportation and corridors

6. Quad (clock tower)

7. Cafeteria

8. Building Security Sensitive Areas (SSA) doors such as IDF’s, computer labs, and asset/equipment storage closets associated with electronic access controlled doors, specifically including but not limited to any associated money handling areas

9. Specific areas where past incidents have occurred and/or future incidents are anticipated to occur, specifically including but not limited to Financial Aid, Check Cashing, Veterans, and Counseling

**Design Standard—Intrusion Detection System (IDS)**

**System Criteria**

1. SCC will deploy industry standard intrusion alarm panels at designated campuses buildings or designated high-value rooms within buildings for the detection and monitoring of unauthorized entry

2. Intrusion alarm panels do not have to be of a single consistent type, this equipment is essentially a commodity and the functionality between various products is similar. However, from the point of view of contractor support and SCC service and maintenance the College should consider standardizing on a single product type

3. Intrusion detection system alarm control panels shall be installed in a locked enclosure with a locked room

4. PIN-code arming/disarming keypad station shall be installed just inside the main authorized user entry door
   a. The keypad station should not be visible from the exterior of the building or room to be protected
   b. The main authorized user entry door associated with the keypad station shall be programmed as an entry/exit delay in the system in order to give the authorized user time to enter and disarm, or exit after arming, the system
c. Do not install a motion detection sensor that covers the area of the keypad station, or the authorized user will not be able to enter and disarm the system without activating the alarm, and they will not be able to arm the system without generating a system fault.

5. Primary alarm signal communication shall be via a telephone line dialer module
   a. SCC shall contract monitoring service for each alarm panel from a UL-Listed 3rd party commercial Central Station monitoring service
   b. Alarm signal communication telephone line shall be a supervised circuit to produce a ‘trouble’ or ‘comm loss’ alarm signal on disruption or loss of the alarm signal communication telephone line
   c. Each alarm panel shall require a dedicated analog telephone line (outside service line, not an analog line out from a digital PBX)

6. Each authorized user shall have their own unique PIN-code for arming and disarming of the system
   a. PIN-codes shall be maintained in a centrally controlled list and changed periodically (minimum annually)
   b. PIN-codes shall be removed from the system on turnover of a previously authorized user; this step should be included in the termination or exit interview HR processes along with retrieving any traditional door lock keys and access control card badge credentials
   c. Alarm panels may be programmed to arm and disarm on schedule in addition to a manual process

**Intrusion Detection System Application Criteria**

Intrusion Detection System equipment, cabling, and sensor devices shall be designed, provided, and installed on the following doors, windows, and rooms for an entire building or a specific interior area to be monitored:

1. Exterior doors leading into the building or area: door position switch alarm contacts
   a. Mounted concealed in the door and frame header rabbet
   b. On certain existing doors surface-mounted door position switch alarm contacts may need to be installed on the interior door and frame header face; installation shall limit the amount of exposed cabling and wiring by using armored flex conduit to a junction box
2. Exterior windows leading into the building or area: glass break detection sensors
   a. Ceiling mounted or wall-mounted

3. Interior rooms and corridors: motion detection sensors
   a. Ceiling mounted or wall-mounted
   b. Motion detection sensors shall be dual-technology type to minimize false alarms: passive infrared (PIR) and microwave (Doppler effect)


Emergency Mass Notification shall be provided, installed, and utilized on SCC campuses in accordance with the communication goals of the President’s Advisory Council on Emergency Preparedness (PACEP). Emergency Mass Notification is more of a series of supporting systems and procedures than it is a single system.

This series of supporting electronic and software-based systems includes but is not limited to:

1. Electronic automated notification message broadcasting services over SMS text/email/phone call trees
2. Indoor public address announcements
3. Outdoor public address announcements
4. Outdoor Emergency Telephones (2-way communication)
5. Indoor and outdoor electronic signage
6. Integration with the campus Cisco VOIP telephone system
7. Integration with the campus Utelogy centralized smart classroom management system

These individual system components should be integrated at a software-based level where possible. These systems should be coordinated with regard to the governing policies and procedures for their use regardless of whether they are integrated or separate individually operated systems. These coordinating policies and procedures should include but not be limited to such factors as:

1. Trigger events for deployment
2. Coordinated messaging
3. Notification statement guidance and pre-written and approved announcements
4. Definition of proper and authorized usage
5. Disciplinary measures for improper and unauthorized usage
6. Guidelines for system deployment sequence, process, and priority

Automated Notification Message Broadcasting Service
Refer to AlertU website https://www.alertu.org/ for more information regarding this hosted service.

Refer to SCC website http://www.solano.edu/ for enrollment information.

Indoor Public Address
Refer to related Design Standards.

Outdoor Public Address
Outdoor public address is produced through exterior mounted broadcast loudspeakers. These loudspeakers should be installed throughout the campus grounds based on a campus-wide strategic layout though they may be installed as part of specific projects. Outdoor public address loudspeakers may be used to broadcast live voice messages, recorded voice messages, or siren sounds. Outdoor public address loudspeakers shall be integrated into the Talk-A-Phone WEBS mass notification platform.

Outdoor public address loudspeakers shall be: School Outfitters AmpliVox Sound Systems Half-Mile Hailer Outdoor Speaker System.

Outdoor “Blue Tower” Emergency Telephones
Outdoor 2-way emergency communication is produced through exterior mounted “Blue Tower” Emergency Telephones. These Emergency Telephones should be installed throughout the campus grounds based on a campus-wide strategic layout though they may be installed as part of specific projects.
Outdoor “Blue Tower” Emergency Telephones shall be: Talk-A-Phone WEBS multi-layer hardware and software mass notification platform. Platform components include: outdoor tower units or wall-mount units. The tower hardware units can be configured to support strobes, cameras, and light fixtures. Tower hardware units shall be provided with supervised communication links and call source announcement capability. The outdoor public address loudspeakers shall be integrated into the Talk-A-Phone WEBS mass notification platform.

**Design Standard— Crime Prevention through Environmental Design (CPTED)**

Crime Prevention through Environmental Design (CPTED) is a design perspective which leverages physical and environmental aspects to incorporate security within a campus.

The four principles of CPTED are:

- Natural Surveillance
- Natural Access Control
- Territorial Reinforcement
- Maintenance and Management

From a high-level perspective, Natural Surveillance would be ensuring that sight lines are open and trees and bushes aren’t obstructing views in strategic areas that could encourage crime or vandalism. The intent of natural surveillance is to increase the perception of observation, which can affect and alter the decision-making process with regard to inappropriate and unauthorized behavior.

Natural Access Control would be the thoughtful application of environmental designs (plants, trees, or benches) used to “control” or “funnel” access to certain areas. For example, properly located entrances, exits, fencing, landscaping and lighting can subtly direct both foot and vehicular traffic in ways that decreases criminal opportunities.

The last two principals – Territorial Reinforcement and Maintenance and Management – are related to invoking a sense of pride and investment within the campus so people feel this campus is their own, which naturally encourages them to protect the space. This is known to be related to reduction in opportunities for aberrant or criminal behavior such as vandalism.

**Approved Manufacturers**

Stanley Security Solutions / BEST Access Systems (EACS)  
Card Access

Luxriot Video Management System (VMS)  
This is just software
DSC MaxSys (IDS)
AlertU (EMNS)
School Outfitters AmpliVox Sound Systems (EMNS)
Talk-A-Phone WEBS (EMNS)

**Substitutes Allowed**
None noted.

**Associated Design Standards and Construction Specifications**

**Associated Design Standards:**
None noted.

**Construction Specifications:**

- 28 10 00 Electronic Access Control and Intrusion Detection
- 28 13 00 Access Control
- 28 16 00 Intrusion Detection
- 28 20 00 Electronic Surveillance
- 28 23 00 Video Surveillance

**Addendum ‘A’**

**Electronic Access Control System Standard**
Electronic Access Control System Standard

Solano Community College understands that there are advantages, efficiencies, and cost savings to be realized with the adoption and ongoing commitment to facilities Standards. In pursuit of these benefits Solano Community College is currently pursuing an initiative for the creation, development, and adoption of Standards. Electronic security systems—including an Electronic Access Control System—are an important part of such Standards.

Standards ensure that Electronic Access Control System installations, retrofits, replacements, and upgrades maintain system consistency and compatibility – regardless of project timing or funding source. Standards also support a single system database to avoid redundancy, duplication, and error, facilitate system administrator training and back-up, facilitate service and maintenance, and act as a record document that can be periodically updated to reflect new developments and requirements.

Ongoing and future renovation projects require timely direction with regard to the selection of the Standard for an Electronic Access Control System. The selected Electronic Access Control System should be purpose-built for access control functionality, support wireless and hardwired access control locking door hardware, support integration with software for the maintenance of the traditional “hard key” Keying System, supported by numerous local competitive contractors, and should not require recurring licensing fees.

Solano Community College hereby selects BEST Access Systems “Stanley WI-Q Technology Wireless Access Management System” including associated system software, equipment components, and electronic locking door hardware as the Standard Electronic Access Control System.

Electronic access control devices shall be installed on all exterior building doors, with the exception of emergency exit only doors with no exterior trim (no exterior lockset knobs/lever handles or key cylinders). These electronic access control devices shall provide wireless or hardwired communication to the standardized centralized access control system software platform. Additional interior doors may be installed with electronic access control devices at the discretion of Solano Community College (such as at MDF/IDF equipment closets, computer labs, classrooms, etc.).

This direction applies to the following facilities:
FAIRFIELD CAMPUS | 4000 Suisun Valley Road, Fairfield, CA 94534
VACAVILLE CENTER | 2001 North Village Parkway, Vacaville, CA 95688
VALLEJO CENTER | 545 Columbus Parkway, Vallejo, CA 94591

End of Document
DESIGN STANDARD FOR FIRE ALARM SYSTEMS

Purpose

The purpose of this document is to standardize the basic elements of the Fire Alarm system design process. The Design Standard has the purpose of creating a consistent application of Fire Alarm system design throughout the Solano Community College (SCC) District, therefore achieving a standard of quality for maintenance and reliability throughout all renovation and new building projects. Deviations from this standard shall be approved by SCC.

Design Standard—Fire Alarm Systems (FAS)

Design standards ensure that the Fire Alarm System installations, retrofits, replacements, and upgrades maintain system consistency and compatibility—regardless of project timing or funding source. These EACS Standards require use of a specific brand (manufacturer) of the FAS, including control panels, alarm initiating devices, and alarm notification devices, to ensure uniformity in alarm reporting, and compatibility with the existing FAS in use on the SCCD campus. The standards will also facilitate service and maintenance, and act as a record document that can be periodically updated to reflect new developments and requirements.

Fire Alarm System Criteria

1. SCCD will continue to utilize a standardized Fire Alarm System at all campus locations, compatible with the existing Fire Alarm systems.

2. For new construction, the contractor shall provide a new Fire Alarm Control Panel (FACP), GE model EST3. The FACP shall be connected to the campus-wide Fire Alarm system network via fiber optic cable using a multi-priority peer-to-peer token ring protocol.

3. The FACP will be programmed to display system status and all alarms at the FACP, and on the existing Fireworks graphics workstations using the EST3 Life Safety Network.

4. All alarms and trouble conditions will also report to the UL-approved 24 hour central station service (Sacramento Valley Alarm) via the existing Digital Alarm Communicator Transmitter (DACT) located inside the Building 1800B FACP.

5. For retrofit/remodel projects, the contractor shall utilize the existing GE EST3 FACP found in each of the existing buildings. All alarm initiating devices and alarm notification devices shall be connected to the FACP in the affected building.

6. For buildings not located on the main SCCD campus, the FACP shall include a DACT connected via phone line to the UL-approved 24 hour central station monitoring service.
7. Consideration should be given to potential future integration of the FAS with the Emergency Mass Notification System (EMNS) when an EMNS is designed and put into place on the SCCD campus.

**Fire Alarm System Design Criteria**

1. All Fire Alarm System (FAS) alarm initiation devices shall be intelligent addressable type, and shall display specific device ID, type, and location on the FACP, and on the FireWorks graphic workstation annunciator.

2. All alarms and trouble conditions will report to the UL-approved 24 hour central station service (Sacramento Valley Alarm) via the existing system dialer located in Building 1800B.

3. The FAS design shall include intelligent manual pull stations at all building exits.

4. The FAS design shall include intelligent photoelectric smoke detectors at all Code required locations.

5. The FAS design shall include intelligent heat detectors at all Code required locations.

6. The FAS design shall include intelligent photoelectric duct-mounted smoke detectors for all supply fans > 2,000 CFM. Provide NEMA-3R enclosures for all duct smoke detectors mounted in exterior and/or exposed locations. Provide fan shutdown upon alarm of the associated duct smoke detector.

7. The FAS shall monitor fire protection (sprinkler) system water flow alarm and valve tamper switches.

8. The FAS shall monitor all auxiliary alarm systems (fire suppression, etc.) as required by Code.

9. The FAS shall provide audible and visual alarm notification throughout the affected building in the event of an alarm. All strobe alarm lights shall be synchronized, and installed in compliance with ADA regulations.

10. All alarms and trouble conditions will report to the UL-approved 24 hour central station service (Sacramento Valley Alarm) via the existing system dialer located in Building 1800B.

11. The Fire Alarm contractor shall be responsible for all required permits.

12. The Fire Alarm contractor shall provide complete system documentation, including product data, associated CSFM listing sheets, and installation shop drawings, and shall submit documentation and obtain approval from the Division of the State Architect prior to the start of construction.
13. The Fire Alarm contractor shall conduct a test and commissioning of the installed system, and shall obtain approval from the Authority Having Jurisdiction (AHJ) prior to building occupancy.

14. The Fire Alarm Contractor and manufacturer guarantee installation, equipment, software, software support and all parts and labor for one year from written notification of acceptance by the Owner.

15. The Fire Alarm contractor shall provide record drawings showing the as-built condition/location of all equipment, devices, and wiring installed on the project.

**Approved Manufacturers**

GE EST3 Fire Alarm Control Panel

Edwards Intelligent Addressable Alarm Devices

Edwards Alarm Notification Devices

System Sensor Alarm Notification devices

**Substitutes Allowed**

None noted.

**Associated Code References and Construction Specifications**

**Associated Code References (current approved issue):**

- ADA – Title 3 of the Americans with Disabilities Act
- CCR – Titles 19 and 24 of the California Code of Regulations
- CBC – 2012 International Building Code with 2013 CA Amendments
- CEC – 2011 National Electrical Code with 2013 CA Amendments
- CFC – 2012 International Fire Code with 2013 CA Amendments
- CMC – 2012 International Mechanical Code with 2013 CA Amendments
- NEMA – National Electrical Manufacturers’ Association
- NFPA 72 – 2010 National Fire Protection Association Standards
- UL – Underwriters Laboratories, Inc.

**Construction Specifications:**

- 28 31 00 Fire Alarm Systems

End of Document