FCMAT
FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
CSIS California School Information Services

Burlingame School District

Technology Review

June 7, 2012

Joel D. Montero
Chief Executive Officer

FCMAT
FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
CSIS California School Information Services

June 7, 2012

Maggie MacIsaac, Ed.D., Superintendent
Burlingame School District
1825 Trousdale Drive
Burlingame, CA 94010

Dear Superintendent McIsaac,

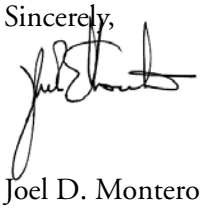
In December 2011, the Burlingame School District and the Fiscal Crisis and Management Assistance Team (FCMAT) entered into an agreement for a review of the district's technology operations. Specifically, the agreement stated that FCMAT would perform the following:

1. Review the district's organizational structure for technology support services and make recommendations for improvement.
2. Review the district's staffing for technology support services and make recommendations for improvement.
3. Review the district's delivery of administrative technology support services and make recommendations for improvement.
4. Review the district's delivery of instructional technology support services and make recommendations for improvement.
5. Conduct an end-to-end network discovery audit to fully document the district's network and identify network elements for replacement/upgrade.
6. Based on the output of the network discovery audit, provide recommendations regarding cabling that needs to be replaced or installed to improve network reliability and performance.
7. Based on the output of the network discovery audit, provide recommendations regarding network elements that need to be replaced, upgraded, and/or installed to improve network reliability and performance.

8. Based on the output of the network discovery audit, create a new wide area network (WAN) design that improves network reliability and performance. These documents shall include a map and description of recommended backbone elements, maps and descriptions of recommended network elements for each site local area network (LAN), and recommended network element configurations.

This final report contains the study team's findings and recommendations in the above areas of review. We appreciate the opportunity to serve the Burlingame School District, and extend our thanks to all the staff for their assistance during fieldwork.

Sincerely,



Joel D. Montero
Chief Executive Officer

Table of contents

About FCMAT iii

Introduction 1

Background 1

Study Guidelines 1

Study Team 2

Executive Summary 3

Findings and Recommendations 5

Network Infrastructure and Administration 5

Technician Support Services 13

Instructional Technology 17

Management, Staffing and Communications 21

Network Discovery Audit 25

Appendices 37

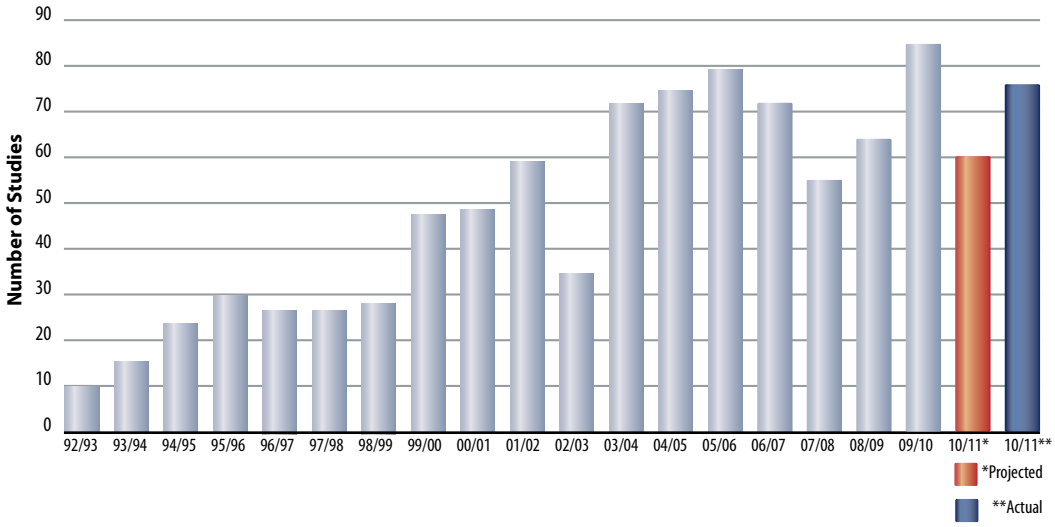
About FCMAT

FCMAT's primary mission is to assist California's local K-14 educational agencies to identify, prevent, and resolve financial and data management challenges. FCMAT provides fiscal and data management assistance, professional development training, product development and other related school business and data services. FCMAT's fiscal and management assistance services are used not just to help avert fiscal crisis, but to promote sound financial practices and efficient operations. FCMAT's data management services are used to help local educational agencies (LEAs) meet state reporting responsibilities, improve data quality, and share information.

FCMAT may be requested to provide fiscal crisis or management assistance by a school district, charter school, community college, county office of education, the state Superintendent of Public Instruction, or the Legislature.

When a request or assignment is received, FCMAT assembles a study team that works closely with the local education agency to define the scope of work, conduct on-site fieldwork and provide a written report with findings and recommendations to help resolve issues, overcome challenges and plan for the future.

Studies by Fiscal Year



FCMAT also develops and provides numerous publications, software tools, workshops and professional development opportunities to help local educational agencies operate more effectively and fulfill their fiscal oversight and data management responsibilities. The California School Information Services (CSIS) arm of FCMAT assists the California Department of Education with the implementation of the California Longitudinal Pupil Achievement Data System (CALPADS) and also maintains DataGate, the FCMAT/CSIS software LEAs use for CSIS services. FCMAT was created by Assembly Bill 1200 in 1992 to assist LEAs to meet and sustain their financial obligations. Assembly Bill 107 in 1997 charged FCMAT with responsibility for CSIS and its statewide data management work. Assembly Bill 1115 in 1999 codified CSIS' mission.

AB 1200 is also a statewide plan for county office of education and school districts to work together locally to improve fiscal procedures and accountability standards. Assembly Bill 2756 (2004) provides specific responsibilities to FCMAT with regard to districts that have received emergency state loans.

In January 2006, SB 430 (charter schools) and AB 1366 (community colleges) became law and expanded FCMAT's services to those types of LEAs.

Since 1992, FCMAT has been engaged to perform nearly 850 reviews for LEAs, including school districts, county offices of education, charter schools and community colleges. The Kern County Superintendent of Schools is the administrative agent for FCMAT. The team is led by Joel D. Montero, Chief Executive Officer, with funding derived through appropriations in the state budget and a modest fee schedule for charges to requesting agencies.

Introduction

Background

Located in the North Bay region of the San Francisco Bay Area, the Burlingame School District serves approximately 2,900 students at five elementary schools and one middle school. With continued growth of Burlingame's student population over the last five years, just short of 20%, and additional projected growth of approximately 5% over the next four years, the district looks forward to the construction of a seventh campus.

The district enjoys the support of numerous volunteers committed to enhancing the educational opportunities of the district's students. Through the Burlingame Community Educational Foundation, parents and community members are committed to raising considerable money and volunteering countless hours as a dedicated effort to support the district's educational programs. Individuals also enrich the learning environment by volunteering in classrooms.

Study Guidelines

The Burlingame School District contracted with the Fiscal Crisis and Management Assistance Team (FCMAT) in December 2011 to conduct a review of the district's operations related to technology. Specifically, the study agreement states that FCMAT will complete the following:

1. Review the district's organizational structure for technology support services and make recommendations for improvement.
2. Review the district's staffing for technology support services and make recommendations for improvement.
3. Review the district's delivery of administrative technology support services and make recommendations for improvement.
4. Review the district's delivery of instructional technology support services and make recommendations for improvement.
5. Conduct an end-to-end network discovery audit to fully document the district's network and identify network elements for replacement/upgrade.
6. Based on the output of the network discovery audit, provide recommendations regarding cabling that needs to be replaced or installed to improve network reliability and performance.
7. Based on the output of the network discovery audit, provide recommendations regarding network elements that need to be replaced, upgraded, and/or installed to improved network reliability and performance.
8. Based on the output of the network discovery audit, create a new WAN design that improves network reliability and performance. These documents shall include a map and description of recommended backbone elements, maps and descriptions of recommended network elements for each site LAN, and recommended network element configurations.

FCMAT visited the district on March 6-7, 2012 to interview employees and collect data. During this visit, team members also toured the McKinley, Washington, and Roosevelt elementary school sites, and the Burlingame Intermediate School site. Prior to the team's visit, a network discovery audit of the district's technology infrastructure was conducted from February 21-24, 2012. This report is the result of those activities.

Study Team

The study team was composed of the following members:

Marisa Ploog, CPA
FCMAT Fiscal Intervention Specialist
Bakersfield, CA

Mike Vincelli*
Director of Technology
Shasta Union High School District
Redding, CA

Robert Black*
FCMAT Consultant
Bakersfield, CA

Laura Haywood
FCMAT Technical Writer
Bakersfield, CA

Executive Summary

Most school districts are challenged by the rapid changes in technology use and support, and the Burlingame School District is not an exception. As reliance on advanced technology increases, so do demands on the resources required to implement, support, maintain and replace these tools. Effective implementation of technology requires a strong, well-structured technology department that is sufficiently experienced to support the district's operations and the integration of technology into the classroom as a means for maximizing the district's academic programs.

The district's technology services department performs a wide range of technology-related duties but struggles to fully support the district's technology infrastructure. The staff has limited experience and technical training, and the department lacks an experienced technology leader. Ineffective communications also contribute to the district's inability to implement, use and support technology. Operational issues that affect the district and sites are not well communicated between technology staff, site staff and district administration. The lack of a formally trained technology leadership position has hampered the district's capacity to establish a well-designed technology department that can guide, implement and support the technologies required for daily operations and classroom instruction. The lack of a clear and formal leadership structure also impedes implementation of the district's vision for technology. The district should hire a formally trained leader to direct a collaborative team that supports the district's curriculum and technology integration needs. Mandates such as common core assessments and the need to provide students, staff and community members with access to network resources make technology services a vital contributor to district operations.

The district network infrastructure is not documented. Network documentation is necessary to successfully manage network operations, enabling technicians and outside vendors to effectively troubleshoot network issues in a timely manner. The district should develop detailed network documentation and ensure that it is routinely reviewed and updated.

An audit of the cabling infrastructure at each site identified deficiencies throughout the district including the lack of secured locations for network equipment with adequate environmental controls; poor planning and workmanship on installation of cabling and patch panels; disorganized equipment racks; lack of network documentation and labeling; inconsistent configurations of the district's network infrastructure devices and insufficient security controls on network routers and switches.

Technology advances in the classroom present technology staff with challenges related to acquisition, configuration, implementation and support. Campus modernization projects completed without well-developed strategic plans for implementation and the lack of experience among technical staff to support the updated technology infrastructure have left the district with costly infrastructure and equipment that is underutilized or not utilized at all.

The district should develop, update and clearly communicate a comprehensive plan that defines the parameters for technology use in all areas, from administrative operations to the classroom. Each area and its environment should be thoroughly reviewed before technology is acquired or implemented for it. The potential benefits of any proposed equipment, software or delivery system and the potential demands that it may impose on the district's current and future resources should be carefully considered.

District staff members frequently commented on performance issues of the technology utilized in the work environment and classroom. The speed of classroom technology was among the issues

experienced by school site staff. FCMAT's research into the contributing factors associated with network speed identified several deficiencies, including:

- Network server and other switch communication issues
- Poorly constructed network structures
- Improper and inconsistent network and computer configurations

The district does not have centralized formal backup, which leaves it at risk of data loss in the event of hard drive crashes, disasters or virus attacks. District staff shared that there is no centralized network location for staff members to save their work, so staff save data to their local disc drives on individual computers. Some staff stated that they back up their data to external devices; however, this is not a district-wide practice. The lack of a formal data recovery plan will make it difficult for technology staff to restore data in a timely fashion. The district should develop and implement a centralized backup system to uniformly back up and store data in an offsite location. This plan should identify all systems utilized by the district that record and/or document critical data.

Many staff expressed frustration with email communications. Although spam filtering is necessary to prevent undesirable junk email from delivery, the district's settings block many essential emails from parents and also block common educational resources such as the California Department of Education. District technicians are not sufficiently knowledgeable in managing the application and thus rely on software default settings to manage email delivery. The district should work with the software provider to modify spam filter settings to ensure valid email communications reach their destinations. Training should also be sought for district technicians to ensure they can manage the systems settings.

The district lacks professional development for both technology users and support staff. The district should assess the skills and abilities of each technician and determine the professional development necessary to ensure they can support the district's technology and instructional software and equipment. Technicians should also be adequately trained to support any new equipment and software that is implemented. Instructional staff should be provided training on all technology equipment in the classroom setting to ensure its effective incorporation into the instructional program.

Findings and Recommendations

Network Infrastructure and Administration

The district's network infrastructure is not documented and has been built without formal planning and design focused on current and future needs. Accurate network documentation is critical to successfully manage any production network and ensure that district technicians or outside vendors can troubleshoot network issues quickly and efficiently. The documentation needs to be reviewed for accuracy and updated regularly. The district network does not include a management system that would provide continuous automated measurement of the network's performance and automated collection and notification of critical network events. Documentation should include switching and routing documentation, server documentation, IP addressing, time sync, passwords, firewall, phone system, wireless, and backup systems.

FCMAT's network discovery audit of the district's network is contained in Appendix E.

Network Configuration

Teachers and staff have little or no online accessible storage to retain data and therefore save files on their local drive. This limits accessibility to these files to a single computer. Storing files on local drives also limits the ability for effective data backup and recovery. Efficient replacement of computers also becomes much more difficult when data is stored on individual computers because the data must be identified and transferred from the old computer to the new computer. Another risk to local storage presents itself if a computer is stolen or the hard drive crashes. In these events any user data is lost and will not be recoverable. Local storage also prevents staff from accessing their files from another district location.

A new server network that incorporates virtualization would allow many servers to operate on one physical piece of hardware, greatly reducing hardware costs. One option would be to centrally locate all servers at the Burlingame Intermediate School, with new fast wide area network (WAN) lines to each school site. Centrally locating servers simplifies network maintenance, service, and backup. A new server network with a district-wide Active Directory structure would allow staff and students with individual logins to access mapped drive storage that would be secure and backed up. A sample Active Directory structure is provided in Appendix A. A centralized server network also provides students and teachers access to their files when they move from site to site, reducing the need for ancillary devices such as USB drives. Although the district utilizes both Apple and PC products, Active Directory can be utilized for Apple products for network authentication and access to shared server storage and user storage with Windows server 2008R2. Shared storage would allow teachers from each site to share Smart Board files and lesson plans. It also would be possible to extend the district's Cisco wireless authentication to groups and students, giving the technology department and district easier, more effective control of wireless access to network resources.

System Backup

Interviews with staff revealed that the district has no formal and only some informal backup procedures to recover lost data from hard drive crashes, disasters or virus attacks. This subjects the district to substantial risk of data loss. The absence of a data recovery plan will make it difficult to restore data or, in the case of a complete server failure, to restore data in a timely fashion.

The district should develop and implement centralized backup for all systems that is stored in an offsite location.

A disk-to-disk backup also is necessary to safeguard critical hard drives and servers. Centralized backup would be best because the district is upgrading WAN lines between sites to 100 MB this summer. With the faster WAN speed it would be possible to back up the entire district at night to a centralized location such as Burlingame Intermediate School. Software such as BackupExec or EMC Networker verifies the integrity of the data being backed up, catalogs the data, and allows quick data recovery. It is a best practice to assign an employee to place the backups in a district safe or bank safety deposit box.

A comprehensive disaster recovery plan identifies all systems that record and/or document critical data. Examples of major technology applications are Internet access, accounting systems, student information systems and email systems. Best practice is to back up all critical systems daily and store the backups offsite in a fireproof location.

Recommendations

The district should:

1. Develop detailed network documentation.
2. Design a new server network that incorporates virtualization.
3. Develop and implement a centralized backup for all systems, with storage in an offsite location.
4. Develop and implement a backup system to safeguard critical hard drives and servers.
5. Develop a disaster recovery plan.

Technology Environment

Many of the wiring closets inspected had inadequate ventilation and/or cooling infrastructure. The heat buildup in these rooms could damage equipment. District wiring closets need proper operational cooling, ventilation and uninterruptible power supplies to ensure the equipment is properly safeguarded against interruption of electrical services, environmental threats and overheating. It is essential for the temperature in these rooms to be maintained between 68-73 degrees. During modernization these rooms need to be on separate small air conditioning systems to ensure they are not turned off during summer months.

Circuits for network closets need to be isolated and dedicated to network equipment, with proper ventilation and cooling to prevent equipment from becoming damaged. Electrical outlets accessible to the same circuit should be controlled to ensure unnecessary devices are not accessing power from these sources.

Recommendations

The district should:

1. Inspect network closets and ensure that circuits are isolated and dedicated to network equipment, with proper ventilation and cooling to prevent equipment from becoming damaged.

Technology Plan

School districts develop five-year technology plans to describe their use of educational technology and to outline the strategic goals for its distribution and use. The plan focuses on the use of technology to support the curriculum and delineates the objectives and strategies for classroom technology, individual student technology, technology required to support school and division operations, and the technology infrastructure. A good technology plan should be grounded in instruction and also includes elements to advance operational efficiency. FCMAT reviewed the district's technology plan for the period of 2008-2013.

The current technology staff did not help develop the current technology plan and were not familiar with its content. The technology plan reviewed did not contain any reference to network design or data safeguard systems in the event of a catastrophic event or security breach. A written plan for system and data recovery is essential in case systems experience catastrophic infrastructure failure, natural disaster, and/or security breaches. The following steps should be taken:

1. Network documentation is needed throughout the network.
2. Document electrical power and air conditioning needs.
3. Create a plan for data backup that includes a backup once every 24 hours both locally and to off-site storage, snapshots for virtual servers four times a day, and monthly backup to be stored in a district safe or bank safety deposit box.
4. Once a year, restore all data from a remote backup to a system that allows comparison and a quality check of the backup. Document and make changes as needed.

The district's documented long-range plans for infrastructure, hardware and software are insufficient. The staff members' lack of technical experience, their isolation from each other on separate campuses and from the staff members responsible for directing the needs of technology significantly handicap the district in supporting technology efforts.

Technology standards for all areas of general operation and school sites should cover the district-wide infrastructure, hardware and software for classrooms and labs. This will help to ensure consistency and equity district-wide and enable technology staff to provide quality, timely support. Financial resources should be identified and allocated and a long-range plan developed to ensure that maintenance and replacement needs can be met. Standards should include statements that detail what hardware, operating systems, and software is supported and for how long.

Recommendations

The district should:

1. Update the technology plan to include procedures for data recovery in the event of catastrophic infrastructure failure, natural disaster and/or security breaches.

2. Develop technology standards for all areas of general operation and school sites.

3. Develop standards based on network equipment capable of handling large school network needs, and avoid technology such as home/office network equipment that is not sufficient to handle these needs.

Hardware and Software

Technicians do not understand the district's purchasing system, how to obtain parts to maintain and repair equipment, or how to charge for these items. Coordinating purchases and using approved vendors could maximize purchasing discounts. Approved vendor lists for each type of acquisition should be based on pricing, availability, support and other purchasing attributes. Technicians need proper training regarding the district's established purchasing process so they can order the items necessary to complete routine equipment maintenance.

The district lacks standard operational policies and procedures for technology acquisitions. Each school site purchases hardware and software without formal standards to guide them. No preventive maintenance or replacement policies exist for operations or programs that depend on technology. Hardware is replaced by school sites when it fails or becomes too old to be effective. Because most technology acquisition and supplemental support comes from individual site budgets, there is a great disparity in equipment type and configurations among campuses.

The district lacks an adequate replacement plan for its technology assets, including its network infrastructure. Although the district continues to expand its use of technology in the classroom, staff reported that no documented equipment replacement plan exists. Standards also are needed for networking equipment, including switches, access points, and wiring.

The district does not provide sites with a list of standardized technology equipment that may be acquired. Such a list would include specifications for the most common types of equipment including teacher laptop computer, teacher desktop computer, district office desktop computer, student computer, classroom printer, etc. Each item specified would be evaluated for quality, the ability to function in the district's network environment, ease of configuration and ability of the technology staff to support it.

A standardized list of common devices can help reduce the time necessary to research and consider each individual purchase requisition. Technology support staff can more easily be trained to configure and support standardized equipment and software.

Although a standardized list of equipment and software can greatly increase efficiencies in purchasing, distribution and support, less common equipment and software requests still need to be considered. When these requests are made, the technology department should be responsible for researching and specifying equipment that is compatible with the district and site infrastructure. Each request also should consider whether the technical ability of staff is sufficient to support the device.

Software is typically purchased with little or no review by the technology services department. The lack of an established software adoption policy and purchasing standards contributes to difficulties in support and system management and results in unsustainable technologies. School site staff need assistance in researching software to determine whether it is compatible with the existing hardware. Software should be standardized as much as possible to keep training costs to a minimum and to obtain the best pricing. Technology and curriculum staff should collaborate on a standard list of software to ensure instructional needs are met. Campuses may utilize varying software applications, but all applications should be reviewed to identify the minimum system requirements necessary to run the software, configuration needs, and the level of support that will be required. Licensing requirements, renewal costs, and the tracking of software inventory and licenses also should be reviewed.

The district does not maintain a software inventory. Many applications limit the number of devices an application may be installed on or accessed at any given time, so the acquisition and installation of software should be tracked district-wide. Measures should be in place to account for software licenses and control installations to ensure compliance with all limitations.

Configurations

The district has not established nor documented standards for system hardware and software configurations, including standard desktop configurations. Three to four configurations should be established for each device. Standard printer configurations should also be defined and utilized. All new technology acquisitions should be received, configured and installed by the technology services department to ensure district-wide standardization.

Recommendations

The district should:

1. Establish standardized technology purchasing practices.
2. Establish an approved vendor list for each type of acquisition based on pricing, availability, support and other purchasing attributes.
3. Ensure that technicians are properly trained in the purchasing process and how to order materials needed for routine equipment maintenance.
4. Establish a list of standardized technology equipment that sites may acquire.
5. Assign the technology department to research and specify equipment models to ensure that acquisitions are compatible with the district's infrastructure.
6. Establish measures to account for software licenses and control installations.
7. Ensure that the technology services department receives, configures and installs all new technology acquisitions.

Email

The district uses a cross-platform email software package, Kerio Connect, as its primary email tool, and four different email retrieval/reading platforms for accessing email: Kerio, Outlook,

Apple Mail, and Entourage. Supporting four platforms makes troubleshooting, training, maintenance and help desk operations difficult. Many staff members complained of slow email performance and difficulties with archiving or easily deleting old emails.

New email systems have integrated email retrieval options. One such platform is Microsoft Exchange server with Outlook. Outlook is supported on both Mac and PC computers and has the same look and feel on both platforms. A single integrated email retrieval platform makes it easier for technicians to maintain and support the email system. While running an Exchange 2010 server can be complex, it is possible to contract for hosted Exchange server services from Microsoft directly or from other vendors. With hosted email services all backup, archive, and spam filtering can be included as a service and maintained by the vendor.

Several mentions were made during staff interviews that the district email spam filter blocks most emails from parents, the CDE and other important sources. During FCMAT's fieldwork, some emails from FCMAT team members were also blocked because the spam filter settings were too restrictive (see message below). Staff reported during interviews that the aggressive settings on the district's spam filter have caused important CDE emails concerning CALPADS and other operational issues to be missed. While the spam is placed in a user accessible spam folder, the users must sift through these emails and identify each email that they want white-listed, which allows future emails to be delivered into the user's email box. This can be very time consuming. The following is an example of the delivery failure notice automatically returned to the sender when an email is blocked through the SPAM filter:

```
Could not be delivered because of

Server refused mail at END OF DATA - 550 Requested action not taken:
email being blocked by BSD Spam Mail Blocker

The following recipients were affected:

gcosta@bsd.k12.ca.us
```

The LightSpeed spam filtering box is a quality product that many school districts utilize for spam filtering. While filtering is necessary to prevent undesirable junk email from delivery, the settings that control the level of blocking should allow legitimate email to be received. District technology staff stated they do not have the knowledge or experience necessary to modify the application settings for email delivery; they simply use the maximum default settings.

Recommendations

The district should:

1. Explore new email system options that have integrated email retrieval platforms.
2. Work with the software vendor to properly modify filter settings to allow school and site business emails to reach their destination.
3. Thoroughly train district technology staff to manage spam filter system settings.

IP Video

During site modernization new IP video systems were installed at two schools. IP video systems allow for the distribution of TV and video through the IP network to classrooms and teachers' PCs. These systems were incorporated into construction plans under the former administration, without the collaboration of technology services. Neither school site administrators nor district technicians understand the equipment, and it is not being utilized.

The district would benefit from determining if the IP video systems installed during modernization are necessary and will be used by the schools. If they will be used, technicians and school staff should be trained in system use and maintenance. Until this determination is made, the district should postpone installation of additional IP video systems during modernization and new construction projects. These systems are very expensive and can be installed after modernization if desired.

Recommendations

The district should:

1. Determine whether the IP video systems installed during modernization are necessary and will be used by the schools. In the meantime, postpone installation of IP video systems during modernization and new construction projects.

Technician Support Services

Maintenance and Replacement Costs

The district does not maintain an inventory of parts and supplies routinely used by technicians to repair equipment. Because there is no clearly established responsibility for the costs associated with technology maintenance including replacement parts (hard drives, projector bulbs, toner cartridges, etc.), technicians struggle to keep classroom technology operational. A list of technology supplies commonly utilized to maintain equipment throughout the district would help ensure that materials are available so technicians can quickly address routine repairs and replacements.

An operational policy that explains who is responsible for the cost of technology repairs, materials, and long-term replacement of network equipment, printers, computers and other items would eliminate the confusion related to purchasing items necessary to complete repairs. For standard equipment, the district should purchase replacement items in bulk to obtain the best pricing. Inventory of replacement parts can be centralized, or group orders can be placed and distributed to individual sites. For example, the district installed a new Smart board in every classroom in the district, so a bulk purchase of projector bulbs would yield a better price. A supply of bulbs could be kept at the district office or at each site for quick and efficient replacement, minimizing instruction downtime. The cost of the inventory could be distributed among sites or charged out as used.

The district may also consider training one or two teachers at each site how to replace projector bulbs because technician support is not available each day. This would minimize downtime for Smart boards, which teachers utilize daily.

Communications

The district's ability to effectively implement and use technology is hampered by ineffective communications between the technology department and other departments and school sites. District staff lacks a clear understanding of project status due to inadequate leadership in the technology department, communication and follow-up on technology projects. The technology department also does not always participate in the planning for modernization and construction projects, making it challenging to implement, configure and support new equipment. Including the technology department in the planning stages of all modernization and construction projects would help ensure that plans and drawings accurately depict the district's existing infrastructure and that all new equipment and infrastructure improvements work with existing technology infrastructure.

The month to month information technology (IT) operational issues that affect the district and sites are not well communicated among technology staff, site staff and district administration. Communication is lacking regarding student data collections and reporting for CALPADS, attendance, and report cards. The absence of a strong, experienced technology leader leaves IT technicians struggling to keep up with daily operations, deadlines and proper communications related to important deadlines that could negatively affect the district if not met.

A district-wide IT operational calendar could help the district meet these deadlines. A sample calendar is provided in Appendix B. A typical calendar would run July to July and list which reports are due and which events need to take place for district operations in each month. Preparing the calendar should be a collaborative activity, with site input. The calendar should be updated in June of each year and should be shared with district administration and site leadership to ensure successful technology operations.

Help Desk

Many of those interviewed expressed a frustration at the lack of a help desk or some form of ticketing/tracking system to acknowledge their request for technological assistance. The district attempted to implement a help desk system in the past, but it was not adhered to by technicians or end users, who continued to email and interrupt technicians who were working on other technology matters. Several sites manage service requests by maintaining a clipboard where staff members record their technology issues. The technicians then utilize these lists to guide their work at the sites each week. This practice bypasses a formal work order system contributing to inefficiencies in prioritization and assignment of work by the technology department supervisor. The lack of a standardized process for managing technology service support requests through a structured help-desk system creates significant inefficiencies in the management of daily technology support duties.

A properly implemented work order system would greatly enhance the tracking and control of work order requests, would allow the technology department supervisor to better organize and prioritize assignments, and would assist in assessing support teams' productivity. Other benefits include improved communication, access to work order status and equipment repair history.

A single project manager should lead the search for an acceptable application and oversee its installation and transition timeline. The transition timeline should be established and communicated district-wide. Users should understand the purpose of the new system and its benefits, should be sufficiently trained in its use, and should be required to use it to request technology support services.

Technician Tools

Staff reported during FCMAT interviews that site technicians often are not equipped with the tools necessary to perform the most basic network troubleshooting. One technician reported using their own personal hard drive duplicator because the district has no imaging software. When asked about tools such as network cable testers and phone test sets, only one technician had a test set and the others thought a cable tester might be available somewhere in the district.

Providing each technician with a tool bag that is equipped with the tools listed below would increase their efficiency in providing routine services. Each technician should be equipped with an inexpensive cable tester and have the ability to check out a phone line test set or larger cable tester from a centralized location for technician tools such as the district office.

Equipment	Position 1	Position 2
Small Phillips #1	x	x
Normal Phillips #2	x	x
Normal Standard	x	x
Small Standard	x	x
7/16 Nut Driver for Projector Mounts	x	
Nut Driver for PC	x	
CAT5 Line Tester		x
CAT5 Stripper	x	
Channel Lock Wrench	x	x
Crescent Wrench	x	x
Electric Probe	x	x
Electrical Scissors	x	x

Flash Light LED	x	x
Gloves	x	x
Level	x	x
Needle Nose Pliers	x	x
Punch Tool	x	x
RJ11 Crimp Tool		x
RJ45 Crimp Tool	x	x
Safety Glasses	x	
Tape Measure	x	
Termination Tool for CAT5/6	x	x
Toner Set	x	x
Utility Knife	x	x
Wire Cutter	x	x
Wire Stripper	x	x

Parts		
Electric Tape		x
Zip Ties	x	
Zip Tie Holders		x
Screws		x
RJ45 Ends	x	
RJ11 Ends	x	x

Recommendations

The district should:

1. Create a list of standard technology supplies commonly used to maintain equipment so that technicians can efficiently address routine repairs and replacements.
2. Establish an operational policy that designates financial responsibility for the cost of technology repairs and materials and long-term replacement of network equipment, printers, computers and other items needed to maintain technology equipment.
3. Include the technology department in the planning stages of all modernization and construction projects to ensure that plans accurately depict the district's infrastructure and that all specified new equipment and infrastructure improvements are compatible with existing technology.
4. Research and implement a help desk system to manage technology service requests.
5. Outfit each technician with a tool bag containing the tools necessary to conduct routine service needs.

Instructional Technology

The Burlingame School District has integrated technology extensively in classrooms for use in instructional delivery. However, school site staff expressed their frustrations regarding the district's approach to technology implementation as well as the adequacy and consistency of support from the technology services department. The district has a mix of technology equipment including Apple and PC products.

Computer Labs

During FCMAT interviews it was shared that PC labs were installed at each school site several years ago over the summer, and that this decision was made without collaborative input from site and technology staff. These computer labs all run at different efficiency levels. Some work well for the students and the instructional program, while others take a long time to log in and run very slowly. FCMAT validated the concerns expressed by staff members at the Washington school site, where the labs and servers are not properly configured. The roaming profiles being used are not properly configured and need to be checked and set up properly. A vendor or school district that has Windows server and XP desktop experience could reimage the PCs and reconfigure the servers to work efficiently. Although the PCs in the school labs are a few years old, they are good quality dual-core machines that should have another year or two of useful life.

While there are PC labs at each site, mobile carts seem to be much more student/teacher friendly in the K-5 environment. Most teachers interviewed by FCMAT favored the use of the mobile carts. However, prior to any change in school site technology supporting the instructional program, a committee of teachers and administrators should collaborate to identify the best options.

Staff shared that students constantly change the desktop configuration settings on the computers in the PC labs. This alters what appears on the monitor, which interferes with the delivery of instruction. Software such as Deep Freeze allows students to fully use the computers even to the point of deleting the operating system, without permanently changing the computer. When this software is utilized, once a student is done using the PC and the computer is rebooted, the original settings are immediately restored. This ensures that each computer is set up and looks the same for each student. It also greatly reduces the demands on technician support for labs.

Professional Development

Nearly all staff interviewed (teachers, technicians, secretaries, principals) expressed concern about the lack of professional development or training in technology. One teacher stated, "I know basically how to use the Smart board, but I don't know how to teach with it." The district should create a professional development plan that includes the student information system (Power School), CALPADS, Windows server and desktop, Lexia software, Smart board, and other hardware and software tools utilized by staff. Technology staff could benefit from attending the California Education Technology Professionals Association (CETPA) conference or other technology conferences, or working with other school districts in the area.

Student Data

During staff interviews it was noted that the district is considering an online student registration system with integration into Power School. While this has been accomplished in many other districts, the skill level of technology staff may make it too ambitious a project for the district to

undertake at this time. Any plan to develop and implement a student registration system should involve a committee of stakeholders to ensure the plan is thorough and considers the needs of system users.

Several administrators noted that Power School's integration with the DataDirector assessment management system does not function optimally. Certain data elements do not transfer properly from Power School into DataDirector. This has caused the administration some concern regarding the accuracy of the data in the assessment program. DataDirector is widely used in public education and is fully compatible with Power School, according to the DataDirector website. DataDirector software support could help determine whether an integration issue needs to be addressed. The issue also may involve data input into Power School.

The district should provide training for site secretaries regarding the importance of the new CALPADS program and why proper data input is critical to accurate student data reporting. The advancement of student data reporting means virtually every keystroke entered into a student information system is uploaded and verified by the California Department of Education via the CALPADS system. Many fields are required for proper CALPADS reporting, and everyone who enters data into the district's student information system should know which data fields are required and why they are important. It is essential to standardize and master the data input that feeds into these reports and ensure that student data is entered timely, consistently, accurately, and to CALPADS specifications. Starting with school year 2012-13, districts could be penalized for not submitting accurate, timely student information through the CALPADS reporting system.

The district does not have a standardized grade reporting system. Teachers create and maintain student report cards in Excel spreadsheets or other applications on their laptop local drives. This does not allow front office staff to reprint report cards for parents. An online report card system would allow teachers and parents to communicate, access, and track student progress online.

Recommendations

The district should:

1. Contract with a vendor or school district that has Windows server and XP desktop experience to reimage the PCs and reconfigure the servers to work efficiently.
2. Establish a committee of teachers and administrators to identify the best options for integrating technology into the classroom.
3. Research and implement a software application that restores original desktop configuration settings when computers are rebooted.
4. Postpone integrating an online student registration system with the student information system until an implementation plan is developed and technology leadership is in place.
5. Develop a professional development plan to implement new technology into the workplace and educational programs.

6. Send technology staff members to CETPA or other technology conferences or to network with nearby school districts as additional sources of training.
7. Provide training to site personnel responsible for entering student information to ensure that data entry is timely, consistent and accurate district-wide and meets CALPADS reporting requirements.
8. Establish a committee to research online grade reporting tools to better communicate, access and track student grades and progress.
9. Work with software support providers to mitigate integration issues that exist between Power School and DataDirector.

Management, Staffing and Communications

The district lacks a technology leader with a clear vision of how the role of technology fits into the overall vision of the district. Over the last several years, district administrators have attempted various staffing restructures in an attempt to resolve problems and improve service and communication in the technology department. However, none of these staffing changes have provided sufficient leadership that is capable of managing the district's technology needs. The absence of a strong, experienced technology leader along with low-performing network systems and lack of progress on technology upgrades has resulted in high levels of end user frustration. Technology staff members that oversee department activities do not have formal education or work experience in technology management that would assist them in managing the rapid growth in district technology usage that has taken place over the past two to three years.

The absence of an experienced, educated IT leader has resulted in poorly defined priorities, minimal project planning, lack of network backups, poor network performance, and insufficient support for curriculum and assessment. Instead of providing proactive, service-oriented support, IT staff members function in a reactive mode that is inefficient and ineffective. This, combined with a lack of communication between technicians and management, has led to considerable mistrust and inability to work as a team.

During IT staff and site staff interviews, staff members were asked if they knew who their supervisor was. Many of the IT staff and some site staff responded that they were unsure. This lack of structure can lead to poor work coordination and/or employee accountability.

An IT manager should be given responsibility for all district technology operations. The manager should oversee the technology staff and communicate with district office administrators and school principals. The IT manager should have an annual budget that he or she helps to create that will support technology department operations.

Four IT employees provide all district technology support. This includes CALPADS reporting and anomaly resolution, and assessment data input/reporting. While these are not traditional IT functions, some school district IT departments perform them because of the complex data import and export and data revisions. The lead technician II position handles these duties. The district has approximately 770 computers and three school site technicians, each of whom provides support to two school sites. Because school sites have varying levels of technology, one technician covers 40% of all school site computers while the other two cover between 29% and 31% of the computers each. The technician supporting 40% of the computers works less than a full-time schedule at six hours a day for 11 months. Two technicians work 12 months at eight hours a day, and one technician works 10 months at eight hours a day. Technician staffing meets minimum requirements at this time, although the district has experienced enrollment growth of approximately 19.62% over the preceding five years and projects an additional 6% over the next five years. With a new school and the implementation of mandated common core standards on the horizon, the district will need to re-evaluate staffing and schedules to continue providing sufficient technical support.

Technicians reported during interviews that they have had little to no training on any of the systems they support and have few resources to consult for help. In addition, some team members do not want to work with the other technicians. A strong leader is needed to identify staff training needs and develop a cohesive team. Strong systems background and networking experience is necessary to ensure that the staff is capable of providing routine service support.

The addition of an IT manager position and an applications support specialist would better serve the district. The position of lead tech II should be eliminated and all support technicians should be at the same level. The IT manager should coordinate and manage all IT systems. This position should guide the district through the rebuilding of the server network and site modernizations that are under way.

Currently, the lead technician II position reports directly to the assistant superintendent/chief business official (CBO). This reporting relationship is fairly common among California school districts. The district's options for organizational models include:

1. Maintain the current reporting line, whereby the IT manager reports to the assistant superintendent/CBO.
2. Place the IT department in the Educational Services division. This could be a good option because most the district technology is used to support classroom instruction. All of the Business Services systems are supported and run by the county office of education.
3. Establish a direct reporting relationship between the IT manager and the district superintendent. This has become increasingly common particularly among large school districts with heavy technology resource implementation and much larger staffing structures for technology.

Recommendations

The district should:

1. Create a technology management position to oversee, guide and communicate the needs of technology.
2. Increase the 11-month, six-hours-a-day position to eight hours a day to handle the workload associated with this position.
3. Eliminate the lead IT tech II position. Assign the duties of this position to a new application support specialist position.
4. Carefully weigh the advantages and disadvantages of aligning IT under Educational Services versus Business Services.
5. Prioritize IT projects and assign technology staff to complete them. Base estimated time to complete projects on input from the IT manager. Add project completion dates to the existing project matrix that can only be adjusted with consent from a district administrator. Conduct a bi-weekly project review by district administrators to ensure continued progress on stated goals.

6. Establish bi-weekly meetings between the IT manager and administration to improve communications. Schedule these sessions for no more than 30 minutes, with the focus on providing updated project information and status of district technology systems.

7. Conduct monthly meetings of the IT manager and school principals to review site-specific issues and discuss any IT projects that affect the school site.

8. Conduct twice-yearly IT staff meetings to discuss staff concerns and issues that may affect classroom instruction. Encourage the sharing of ideas and new technologies that may be useful to the district's staff and students.

9. Develop an organizational chart showing the direct chain of command for each technology position so that employees know who to contact when their immediate supervisor is out of the office.

Network Discovery Audit

Cabling

FCMAT engaged the services of Advanced Data Communications (ADC) to thoroughly examine the cabling infrastructure at the district office and each school site. For each location, ADC created a site map (Appendix E) that identifies existing network cabling, data drops and other infrastructure throughout the location, and an inventory list (Appendix F) of network elements and how they are labeled. For each location ADC also documented deficiencies that should be addressed by the district and made recommendations for resolving these issues (Appendix G). Since the appendices address specific findings and recommendations, they can be referred to for details. This section will summarize the findings and recommendations.

Technology staff utilize network equipment racks to manage telecommunications wiring and connections to workstation devices throughout the district. These racks are commonly referred to as IDF/MDF (intermediate distribution frames/main distribution frame). At most sites, IDF/MDF is not in a closed, secured room. In some locations the switches are placed inside closets rather than a suitable rack or enclosed box designed to house this type of equipment. Some network equipment is located and exposed in high traffic areas. MDF/IDF locations should be in secure areas where equipment cannot be tampered. Locations should be locked and provide adequate environmental controls including ventilation and climate control to prevent equipment from overheating.

Cabling appears to be an afterthought at each site. Site inspections showed that little planning has been done to identify where cable and patch panels should be located. Much of the work was completed incorrectly. Examples of inconsistencies and deficiencies include:

- Patch panels are in two different locations; some are in the wall
- Old cables are still in rack and behind some of the wall plates
- Some cables are CAT5; some are CAT5e
- Indoor cable was used outside, resulting in deteriorated cabling and loose connections
- Cable is more than the standard length (298 ft.)
- Cables coming from the location going to IDF are plugged directly into switch
- Cables are pinched on the pathway by zip ties
- Materials used on pathways are not to code

The district has an opportunity to resolve many of the deficiencies through its campus modernization projects by factoring network cabling and power needs into the remaining modernization projects. Areas that should be addressed in modernization plans include:

- Relocating and securing equipment racks (MDF/IDF)
- Providing adequate power and environmental controls for equipment
- Providing sufficient rack space for equipment and cable management
- Removing all CAT5 cabling, and replacing it with CAT6 or better cable
- Removing all abandoned cabling and patch panels

Technology infrastructure deficiencies could have been prevented through proper planning. For sites that have already gone through modernization, the district should seek opportunities to correct the existing issues. In some cases a contractor may need to perform the work to correct the deficiencies. However, some issues can and should be resolved by district IT staff.

Equipment in MDF and IDF racks is not organized, which complicates troubleshooting and/or locating cables. Components of the network such as patch panels, switches, and fiber panels should be organized in standard positions to ensure technicians can efficiently address problems as they occur. Specific issues include the following:

- Patch cables are too long, bunched and tangled, so technicians must weed through them to find the correct cables and address issues.
- Patch panel, cables, faceplates and jacks are not labeled, which makes it difficult to find where a cable in the network equipment rack is plugged in.
- No map in IDF. A map would allow the technician to see which network plugs are in each room without having to physically go into the room to look.

The following tables are sample standards formats that specify the order in which equipment, patch panels and cable management is installed in the racks, cabling standards such as patch cable length and color, and equipment and cable labeling:

Equipment Rack Cable Standard (Sample)		
Endpoint	Color	Length
Workstation	Yellow (CAT5e or better)	2 ft.
IP Phone	White (CAT5e or better)	2 ft.
Access Point	Purple (CAT5e or better)	2 ft.
Network Device	Orange (Fiber, CAT5e or better)	4 ft.

Equipment Rack Standard (Sample) ***based on a standard 12u equipment enclosure**
Fiber Patch Panel
WAN Router
Cable Management
Copper Patch Panel
Cable Management
Switch
Copper Patch Panel
Cable Management
Switch

McKinley Elementary School IDFs are connected over copper. However, fiber connections between the network equipment racks would enable longer cable runs, higher throughput and less signal loss. The district has fiber running between network equipment racks at most of the schools, so this appears to be an exception.

Terminated fiber cable remained in several locations between IDFs, which may affect network performance.

Recommendations

The district should:

1. Provide a secure area for the MDF/IDF on all sites, including the district office, to ensure equipment is properly safeguarded against tampering and environmental factors.
2. Address deficiencies in cabling and power in future modernization plans, and factor these needs into the remaining modernization projects.
3. Develop a plan to address the deficiencies identified, which at a minimum should include the following items:
    - Purchase patch panels so that cables can be punched down, rather than being directly connected to network equipment.
    - Purchase cable management equipment and Velcro strips to properly secure cabling.
    - Remove abandoned cables as the opportunity arises.
4. Develop a district standard that specifies the order in which equipment, patch panels and cable management are installed in the racks.
5. Establish standards for cabling such as patch cable length and color.
6. Establish standards for equipment and cable labeling.
7. Post established standards in each MDF/IDF location along with site floor plans for faster cable identification and troubleshooting.
8. Pull terminated fiber cable between IDFs to improve network performance.

Local Area Network (LAN)

During interviews, staff at McKinley School reported that student lab computers were very slow. FCMAT assessed lab computers and noted they took more than seven minutes to boot and become operational. FCMAT reviewed the configuration settings and found that the switches were connected on fast Ethernet ports. Lab computers were plugged into HP switches, while staff computers, phones and access points were connected to Cisco switches. Both the HP and Cisco switches support small form-factor pluggable modules, which would allow the switches to be connected at gigabit.

Dynamic Host Configuration Protocol (DHCP) is an application that dynamically assigns IP addresses to network devices like computers, rather than having someone manually assign them. DHCP scope is a range of IP addresses that can be used for dynamic assignment. Typically, DHCP runs from a central server, and all the DHCP scopes are managed from one place. The district does not run DHCP from a server; instead, technicians configure DHCP scopes for network devices like workstations, wireless clients and phones on network equipment. In addi-

tion, DHCP scopes are configured on multiple devices for different aspects of the network. MDF switches have data and IP-phone scopes configured, and routers have user, lab, access point and wireless scopes.

All schools have Windows servers supporting the computer labs. DHCP scopes could be configured on these servers to support subnets on the respective school campuses. Moving DHCP scopes from individual network devices to existing servers would enhance the technician's ability to manage the technology at their respective sites, and would allow them to improve their skills.

Configurations between the district's network infrastructure devices are inconsistent, including those between routers and switches. These inconsistencies are primarily because engineers or companies utilized their own methods to configure devices while installing Cisco network infrastructure devices and phone system rather than following district guidelines. Staff stated that although AT&T was the primary vendor contracted to install the network infrastructure, various subcontractors performed the installations. While this study does not include a comprehensive configuration audit, some of the differences in configurations include:

- Hostnames
- Use of enable and enable secret
- Simple Network Management Protocol (SNMP) configuration
- Console and remote access configuration

Standards for device configuration would include naming and addressing conventions and a security framework that fits the organization. Once standards have been established for device configuration, all future configurations can be done using that framework. A sample configuration standard is provided in Appendix D.

The district has insufficient security controls on its network routers and switches. While the network devices natively support security features to protect from unauthorized access and network problems, many of these features are not enabled on the devices. While this study did not include a comprehensive security audit of the network devices, some of the weak security features currently enabled include:

- Enable password – Network switches use the older enable password command, which uses a weak encryption algorithm.
- No Management ACLs – No access control lists are configured to prevent hosts from attempting to connect to network devices from any location on the network.
- Telnet Management – Both vty and tty lines allow an administrator to connect to network devices for management. Telnet is enabled on device vty lines, allowing for unencrypted device management over the network.
- HTTP Server Enabled – Allows remote hosts to manage device configurations using a web browser.

Network security is vital to any network, and is often assessed separately. The primary security emphasis for this assessment was on the network elements that provide access to endpoints including switches, routers and firewall. Many of these elements are manufactured by Cisco Systems, and many documents are available on the Internet cover device hardening. Hardening is the process of making a device more secure by disabling unsecure features and utilizing other security features to prevent unauthorized access. District technology staff can employ any avail-

able security feature that applies to the district's network environment by accessing the Cisco Guide to Harden Cisco IOS Devices at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#aaa

All unsecure network protocols used for network device management, such as Telnet and HTTP, should be disabled. Protocols such as SNMP should be configured properly to prevent unauthorized access to the network devices. In addition, access control lists prevent network devices from being managed from anywhere in the district. Device management should be restricted to a single subnet on the district's WAN, and to a few hosts.

The Burlingame Intermediate School campus has a Cisco Secure ACS server that is only being used to provide 802.1 x authentications for clients that connect to the wireless network. District technology staff can use the Cisco Secure ACS server for authentication, authorization, and accounting on network devices. This would allow the district to create a management account for all network devices in one location. If changes need to be made to the account, they are made on the ACS server rather than at each device. More information pertaining to Cisco Secure ACS network access restrictions can be obtained at this link: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_tech_note09186a0080858d3c.shtml

The district lacks an updated network equipment refresh plan. Staff referred FCMAT to the district's Education Technology Plan for the years 2008 – 2013. While the document states that the plan will be reviewed annually, there is no indication that it has been reviewed and updated since it was created. Technology staff stated that they did not play a role in developing the current Education Technology Plan and that no updates have been done.

Education technology plans should be reviewed and updated annually because rapidly changing technology shifts the priorities. A network equipment refresh plan should be included in the district's plan. This network equipment refresh plan should be reviewed annually to ensure that devices approaching the end of their useful life are identified and a plan is established for their replacement. The district's network infrastructure was upgraded in early 2009, with most switches and routers replaced. Several of those devices have already reached the manufacturer's (Cisco's) end of life date, and Cisco has established dates for phasing those devices out of support. The district does not have an established plan for replacing devices before they reach the point when service contracts can no longer be renewed. The service contract renewal periods for devices managed by the district are provided below and may be accessed through the links provided.

	End-of-Life Date	End of SW Maintenance Release Date: HW	End of Service Contract Renewal Date: HW
Cisco Catalyst 3750 and 3560 switches	Jan. 4, 2010	July 4, 2013	Sept. 30, 2014

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/end_of_life_notice_c51-574778.html

	End-of-Life Date	End of SW Maintenance Release Date: HW	End of Service Contract Renewal Date: HW
Cisco 2800 Series Integrated Services Router	Nov. 1, 2010	Oct. 31, 2014	Jan. 30, 2016

http://www.cisco.com/en/US/prod/collateral/routers/ps5854/eol_c51-631228.html

	End-of-Life Date	End of SW Maintenance Release Date: HW	End of Service Contract Renewal Date: HW
Cisco 4400 Wireless LAN Controller	Dec. 13, 2010	June 12, 2014	Sept. 8, 2015

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps6366/end_of_life_notice_c51-634665.pdf

	End-of-Life Date	End of SW Maintenance Release Date: HW	End of Service Contract Renewal Date: HW
Cisco 4400 Wireless LAN Controller Module	Oct. 24, 2011	April 23, 2013	July 19, 2016

http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps6730/end_of_life_notice_c51-691054.html

	End-of-Life Date	End of SW Maintenance Release Date: OS SW	End of Service Contract Renewal Date: OS SW
Cisco ASA 5510 Software Release 8.0l	Aug. 23, 2011	Feb 20, 2013	May 18, 2016

Hardware is still supported, but the software running on the device is end of life

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/end_of_life_c51-682452.html

The district has no backup archive of its network devices. During interviews district technical staff recalled a recent failure of a wireless module in a router. Because there was no backup of the configuration, the device had to be rebuilt from sample configurations on other devices.

Device configurations should be regularly backed up and archived in a secure, accessible network location. Device configurations should also be backed up before new configurations are made, to ensure easy roll-back if mistakes are made.

The district lacks a documented disaster recovery plan. A plan is necessary to ensure business continuity in the aftermath of a disaster. The plan should be reviewed annually to ensure that all critical systems, procedures and response teams are updated. Team members should also annually simulate disaster scenarios to identify and correct deficiencies in the plan. The disaster recovery plan should address the following items:

- Identify critical systems and data (payroll records, accounting records, student records, equipment inventory, policies and procedures, etc.)
- Define response team and their individual responsibilities
- Off-site and on-site data and media storage
- Computer recovery facilities (hot sites)
- Recovery plan

The district purchased Cisco SmartNet maintenance contracts for multiple Cisco phones and access points. These contracts are unnecessary and costly. SmartNet for a single IP phone and Access Point would allow Technical Assistance Center (TAC) cases to be opened with Cisco, or software updates can be downloaded. It would be much more cost effective for the district to purchase a spare of each device in the event that a unit fails.

During interviews, technology staff stated that the district plans to upgrade the county connection from 100Mbps to 250Mbps to address issues with poor network performance. As previously mentioned in WAN findings, testing determined that the performance problems being experienced by the schools are related to the configuration of lab servers and workstations, and not the WAN or county office connections. Upgrade in connection speed will not resolve poor network performance and would be an unnecessary expense. The issues raised by staff concerning slowness are local network issues and are unrelated to the Internet connections. Additionally, the district firewall, Cisco ASA5510, is not capable of passing 250 MB of data in and out with 100 MB interfaces. The following link provides information regarding this device: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

The district utilizes a Cisco 7206VXR router to connect to the county office of education. The use of this router is not necessary because when the school district upgraded the WAN and county connections to OPT-E-MAN, Cisco 3750ME switches were installed to support the new connections. While the Cisco 7206VXR router previously was required for the county connection, changes in the network infrastructure provide better alternatives. Connection to the county office should be moved to the newer Cisco Catalyst 3750ME switch, and the Cisco 7206VXR router should be removed from the design. This change would require some new configuration to be performed on the 3750ME switch but would simplify the design and remove a potential point of failure from the network. The district could also cancel the SmartNet maintenance agreement and save money.

Recommendations

The district should:

1. Remove DHCP scopes from individual network devices and configure local DHCP servers to enhance the ability of technicians to manage technology at sites.
2. Develop and maintain written standards for network device configurations that include device naming conventions, management methods, configuration settings and security requirements.
3. Access the Cisco Guide to Harden Cisco IOS Devices, to obtain security features that apply to the district's network environment. Disable all unsecure network protocols used for network device management.
4. Ensure that protocols such as SNMP are configured properly to prevent unauthorized access to the district's network devices.
5. Review and update the Education Technology Plan annually.
6. Establish a plan for replacing devices prior to the end of the service contract.
7. Establish a backup archive for all network devices to ensure that established configurations are preserved and available should a failure occur and reconfigurations become necessary.

8. Develop and document a disaster recovery plan. A sample plan is attached as Appendix H.
9. Discontinue the practice of purchasing and/or renewing multiple Cisco SmartNet maintenance agreements. Use the cost savings for replacement/ spare devices.
10. Cancel the upgrade of the county office of education connection. Move the connection to the newer Cisco Catalyst 3750ME switch installed during recent upgrades and reconfigure appropriately.
11. Remove the Cisco 7206VXR router from the district's network design.
12. Discontinue SmartNet maintenance agreement associated with the Cisco 7206VXR router.

Phone System

The district's voice servers have not been patched or upgraded since they were installed. The Cisco Voice over IP (VoIP) system was installed in 2009. The system has six servers providing call control, voicemail, enhanced 911 and conferencing services. These servers should be upgraded to the latest supported version for the hardware the system is installed on. The district technical staff has little experience with the VoIP system other than basic adds/moves/changes.

The district does not have an equipment refresh plan for its telecommunication systems. District technology staff expressed their lack of knowledge pertaining to the system during interviews. There was no indication that the district has developed a plan to keep the hardware and software maintained. The ongoing maintenance and replacement of VoIP system equipment should be included in the Education Technology Plan. While the system was upgraded in 2009, Cisco has made numerous changes to the product since then. Most of the software installed on the servers has already reached the manufacturer's end of life, and Cisco has established dates for phasing that software out of support. The district should have a plan to refresh these systems, including both hardware and software, before the point when service contracts can no longer be renewed.

	End-of-Life Date	End of SW Maintenance Release Date: SW	End of Service Contract Renewal Date: SW
Cisco Unified Communications Manager 7.1	Dec. 23, 2011	June 22, 2013	Sept. 18, 2014

http://www.cisco.com/en/US/partner/prod/collateral/voicesw/ps6788/vcallcon/ps556/end_of_life_notice_c51-695269.html

	End-of-Life Date	End of SW Maintenance Release Date: SW	End of Service Contract Renewal Date: SW
Cisco Unity Connection 7.1	Dec. 23, 2011	June 22, 2013	Sept. 18, 2014

http://www.cisco.com/en/US/partner/prod/collateral/voicesw/ps6789/ps5745/ps6509/end_of_life_notice_c51-695712.html

	End-of-Life Date	End of SW Maintenance Release Date: SW	End of Service Contract Renewal Date: SW
Cisco Emergency Responder 7.0	April 12, 2010	Oct. 11, 2011	Jan. 6, 2013

http://www.cisco.com/en/US/partner/prod/collateral/voicesw/ps6789/ps7046/ps842/ps9746/end_of_life_notice_c51-588829.html

	End-of-Life Date	End of SW Maintenance Release Date: SW	End of Service Contract Renewal Date: SW
Cisco MeetingPlace Express	Oct. 31, 2009	May 1, 2011	July 27, 2012

http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps6730/end_of_life_notice_c51-691054.html

Voice servers have not been backed up since they were installed. Backups were configured by the vendor, who performed manual backups when the servers were initially configured, but no scheduled backups were configured afterward. The voice servers should be backed up to a network server or workstation running secure file transfer program (SFTP) software. Free SFTP software can be downloaded and installed on most windows platforms. These SFTP servers are supported and recommended:

- Open SSH—for Unix systems
- Cygwin—http://sshwindows.sourceforge.net/
- Titan—http://www.titanftp.com/
- GlobalSCAPE EFT Server, formerly known as GlobalSCAPE's Secure FTP Server

The enhanced 911 system, Emergency Responder, has not been maintained since it was initially installed. It is not clear if the system is providing its intended function. Emergency Responder is supposed to identify the specific location a 911 call was placed from including the address, building and room. Unless a clear purpose and design can be demonstrated and district staff is trained to maintain the system, it does not need to remain on the network. Removal of the Emergency Responder server will allow the address of the location where the 911 call originates to be determined from the local gateway, letting responders know where to go. District staff should consult a qualified Cisco Partner that understands Emergency Responder before deciding whether or not to keep this system.

The district installed but has never used a MeetingPlace Express server that enables audio, video and web meetings. A clear purpose and design should be demonstrated to justify the need for the server. If the server is to be kept, district staff should be trained to maintain the system. Otherwise, it can be removed from the network. Staff should consult a qualified Cisco Partner that understands MeetingPlace Express before deciding whether or not to keep this system.

During interviews, site personnel stated that that caller identification on the phone system is not programmed to identify each school site by its proper name. For example, when a call goes out from the district office its caller ID says Burlingame Intermediate School. This causes parent confusion as to where their return calls should be directed. Another user stated that the voicemail message playback is too fast, and they are unable to get all details on the first pass. FCMAT also discussed changes to the current dial plan with district technicians, where it became apparent that they do not know how to change system settings. IT staff should be adequately trained on the features and functions of the VoIP system so they can perform routine maintenance tasks.

Until district technical staff gain knowledge of the VoIP system, the district will need to contract with a reputable Cisco vendor who is certified in VoIP to address configuration and programming issues. The district should also establish a relationship with a Cisco Partner to assist in more complex configuration tasks.

FCMAT found that staff members at Washington Elementary use two different systems for paging. Site staff utilize the newer Cisco phone system for zone-based paging, and an old phone is kept at the front office for All page. After further investigation, it was determined that the installation of the new phone system was not completed, and the old system was left online for a single phone to perform pages. The secretaries indicated that intercom and paging works differently at all sites. The new Cisco phone system should be configured to interface with the All paging system, and the old phone system retired. The hardware and configuration time required to complete the task should not be significant, but the district should also establish a relationship with a Cisco Partner to assist with this.

Recommendations

The district should:

1. Contract with an experienced Cisco Partner vendor to upgrade the Cisco Voice over IP system to the latest supported version.
2. Include the VoIP system hardware and software refresh plans in the Education Technology Plan.
3. Back up the district voice servers to a network server or workstation running SFTP software.
4. Consult with a qualified Cisco Partner to determine whether the Emergency Responder server should be removed.
5. Consult with a qualified Cisco Partner to determine whether there is a need for the MeetingPlace Express server. In the absence of an identified purpose, remove the server from the network.
6. Send technical staff to basic administrative training for the VoIP system to enable them to perform routine maintenance tasks.
7. Establish a relationship with a Cisco Partner to check all trunk access lines, review and reconfigure the caller ID programming, and assist with more complex configuration tasks related to the VoIP system.
8. Configure the Cisco phone system to interface with the All paging system, and retire the old phone system.

Wide Area Network (WAN)

The Burlingame WAN was upgraded from frame relay to OPT-E-MAN in November 2008. OPT-E-MAN is a switched Ethernet service that connects the schools over AT&T's optical network infrastructure. The OPT-E-MAN network is a very reliable and scalable service to interconnect the school sites. Based on the findings presented by Advanced Data Communications,

the WAN does not need to be redesigned to improve reliability and performance. OPT-E-MAN can be rescaled in the future based on the district's needs.

Technology staff shared that the district plans to upgrade the AT&T WAN connections to each of the sites to address poor network performance. The Washington, Lincoln, McKinley and Roosevelt elementary school sites all currently have 10Mbps WAN connections, and both Franklin Elementary School and the district office have 20Mbps WAN connections. The plan shared with FCMAT is to upgrade the WAN connections to 100Mbps for every location to improve network performance. On a visit to one of the schools (McKinley), FCMAT did some testing in one of the computer labs. The testing showed that the performance problems were with the configuration of the lab server and workstations, and not the WAN connection. Because the district WAN is adequate and redesign is unnecessary, the technology department should focus on ensuring that the server hardware is adequate and configurations are correct. Although an upgrade of WAN lines to 100 MB could provide faster communication between sites, the district would be better served by using the funds associated with that upgrade to update outdated servers and aging workstations.

Although FCMAT did not review WAN fiber and uplink ports for duplex and speed issues, the team believes there may be some problems between sites, servers and other switches communicating with one another via 10/10/1000 speed due to different manufacture type. The district should check each router and switch for proper duplex and speed adjustment between switches, routers, and servers. This will ensure that each piece of network equipment is performing at the speed expected and will deliver a more reliable network.

The district does not have current diagrams of the network. Network diagrams presented by district staff were created in November 2008 by Eaton and Associates, and there is no indication they have been updated.

Recommendations

The district should:

1. Ensure that server hardware is adequate and configurations are correct.
2. Create updated network diagrams to reflect all existing LAN and WAN devices and connection types.

Appendices

Appendix A - Active Directory Structure Example

Appendix B - Sample IT Calendar

Appendix C - Sample Job Descriptions

Appendix D - Sample Configuration

Appendix E - Network Mapping Diagrams

Appendix F - Network Label Inventories

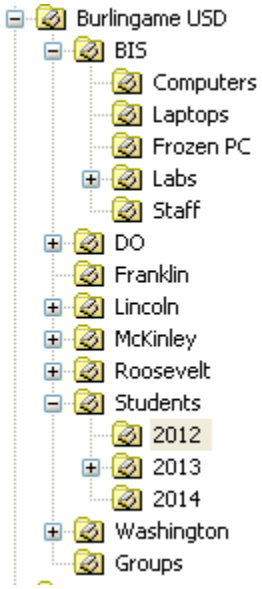
Appendix G - Network Discovery Audit Findings and Recommendations

Appendix H - Sample District Disaster Recovery Plan

Appendix I - Study Agreement

Appendix A
Active Directory Structure Example

Implementing an active directory domain would give the district the ability to assign individual logins to students and staff. With these individual logins, group associations could be used to assign security to shared storage between grades and departments for lesson collaboration, wireless access, content filtering access, private user storage on servers, and a host of other controls that would help maintain the network. Student IDs could be assigned from Power School based on Power School student ID numbers or another ID-based nomenclature. The student IDs would be placed in an organizational unit that would coincide with the student's graduation year. This gives students access to their files, no matter which school they attend in the district. After the students graduate, the organizational unit can simply be deleted.



Appendix B

IT Calendar
Operational Events List 2011-12
High School/Middle School
EXAMPLE

JULY 2011

Enter/update all pertinent student data – Site
Run Query – Missing Pre-Id Data
1 End of Course Exam Results posted in Datawise – DO
14 New year rollover – DO
26 Charter Movement Attendance Reports for previous year - DO

AUGUST 2011

Anomaly Resolution – Ongoing – DO
10 Finalize Master Schedule – Site
15-16 Count of Locator cards not picked up – Site
16 Drop all no-shows by end of day – Site
19 Run Attendance Audit Report - Site
19 Finish entering any missing student data – Site
Run Query – Missing Pre-Id Data
26 Run Enrollment Audit Listing and Students Actively Enrolled in Two Schools reports; send to schools to resolve problems – DO
26 Run Students with less than N period report for students with less than 6 classes - Site
26 Request SSIDs for new students – DO
31 Deadline for October CAHSEE Pre-ID – DO
31 Enrollment Numbers – DO

SEPTEMBER 2011

Anomaly Resolution – Ongoing – DO
CalPass submission – DO
Fitnessgram Import – DO
Import data from SEIS – DO
Import data from Schoolhouse – DO
2 Send list of students dropped and where to since last day of school in June to Superintendent – Site
2 Identify students in various attendance programs (Sped Prog 2, College Connection, CalSafe, etc.) – Site
2 Run Attendance Audit Report; send to IT Dept. by 4 p.m. – Site
2 Enter students in programs such as GATE, Migrant Ed, Homeless, CAHSEE Intensive Instruction. (reference -Aeries Procedures for Registrars and Counseling Secretaries)
9 First quarter deficiency notices, comprehensive schools – Site
9 First ADA month ends ***due to DO 9-14, 4 p.m. – Site***
12 CALPADS Uploads – DO
22 First session report cards, alternative ed – Site
26 CALPADS Uploads – DO

28 Review Exit Reasons and Summer Withdrawal reasons for 10-11 - Site
28 Verify and finalize all graduate data - Site
30 Enrollment Numbers – DO

OCTOBER 2011
(Oct. 5 - Dec. 14 - CALPADS Fall 1 Enrollment/Grads/Dropouts Submission Window - DO)
(Oct. 5 - Jan. 18 - CALPADS Fall 2 Staff/Course/Section Submission Window)

Anomaly Resolution – Ongoing – DO
4-5 CAHSEE Testing – Site
5 CBEDs day/Census Day
5 Run Attendance Audit Report – Site
7 Second ADA month ends ***due to DO 10-12, 4 p.m. – Site***
7 First quarter report cards, comprehensive schools – Site
10 CALPADS Uploads – DO
12 Work on Fall 1 (*SENR, SINF, SPRG*) submissions resolving all fatal errors
15 MAA File - DO
24 CALPADS Uploads – DO
31 Enrollment Numbers – DO

NOVEMBER 2011

Anomaly Resolution – Ongoing – DO
4 Run Attendance Audit Report – Site
4 Third ADA month ends ***due to DO 11-11, 4 p.m. – Site***
4 Second quarter deficiency notice, comprehensive schools – Site
7 CALPADS Uploads – DO
9 Second session report cards, alternative ed – Site
28 CALPADS Uploads – DO
30 Enrollment Numbers – DO

DECEMBER 2011

Anomaly Resolution – Ongoing – DO
2 Run Attendance Audit Report – Site
6 Send Fall 1 reports to sites and district for review
1.1 *Enrollment Primary Status by Subgroup*
1.6 Graduates and Dropouts by Subgroup
1.9 Completers and Dropouts Count
2 Fourth ADA month ends ***due to DO 12-9, 4 p.m. - Site***
8 October CAHSEE Results available – DO
12 CALPADS Uploads – DO
13 First semester report cards, comprehensive schools – Site
14 Fall 1 Certification Deadline
14 P1 report – DO
22 Enrollment Numbers – DO
30 Load 8th grade feeder school data – DO
30 Fifth ADA month ends ***due to DO 1-5, 4 p.m. – Site***

JANUARY 2012

Anomaly Resolution – Ongoing – DO
Work on Fall 2 submissions (SDEM, SASS, CRSE, SCSE) resolving all fatal errors
STAR Writing Pre-ID file due – DO

1 Counselors/Admin to set pre-registration timeline for 2012-13 school year **(must be complete by 4/13/12)** - Site
Preregistration for 12-13 school year begins – Site

3 Deadline for February CAHSEE Pre-Id file due - Site

3 Run Attendance Audit Report – Site

6 Run Enrollment Audit Listing and Students Actively Enrolled in Two Schools reports; send to schools to resolve problems - DO

6 Projected course offering list for 2012-13 due to Instructional Services for approval - Site

9 CALPADS Uploads – DO

10 Send CALPADS Fall 2 reports to sites and district for review
2.4 English Learner Education Services-Student Count Unduplicated
2.5 English Learner Education Services-Unduplicated Count of Teachers Providing EL
3.4 NCLB Core Course Section Compliance-Count by Content Area
3.6 Course Section Enrollment-Count by Content Area
4.1 Staff Count and FTE by Job Classification

13 Third session report cards, alternative ed – Site

13 Run Students with less than N period report for students with less than 6 classes – Site

18 Fall 2 Certification Deadline

23 CALPADS Uploads - DO

27 Run Attendance Audit Report -Site

27 Sixth ADA month ends ***due to DO 2-3, 4 p.m. – Site***

31 Enrollment Numbers - DO

FEBRUARY 2012

Anomaly Resolution – Ongoing – DO

1 Run Query – Missing Pre-Id Data and enter any missing data -Site

4 STAR Pre-Id file due MC – DO

4 Third quarter deficiency notices, comprehensive schools – Site

8 CALPADS Uploads - DO

7-8 CAHSEE Testing - Site

21 CALPADS Uploads - DO

24 Run Attendance Audit Report -Site

24 Seventh ADA month ends ***due to DO 2/29, 4 p.m. – Site***

29 Enrollment Numbers - DO

MARCH 2012
(March 1 - 28 - CALPADS EL Counts Immigration Status Submission Window)

Anomaly Resolution – Ongoing - DO

2 Fourth Session report cards, alternative ed - Site

5 CALPADS Uploads – DO

10 Send Spring 1 Reports to Sites and District for Review
2.1 Title III Eligible Immigrants-Count
2.8 English Language Acquisition Status-Count by Primary Language

2.9 English Language Acquisition Status-Census Comparison
2.12 English Language Acquisition Status-ELs Reclassified RFEP
16 Third quarter report cards, comprehensive schools – Site
19 CALPADS Uploads - DO
23 Run Attendance Audit Report - Site
23 Eighth ADA month end ***due to DO 3-28, 4 p.m. – Site***
30 Run Tally of Course Requests –Site
30 Enrollment Numbers - DO

APRIL 2012
Anomaly Resolution – Ongoing – DO
2 CALPADS Uploads - DO
4 Deadline for May CAHSEE Pre-Id file due – DO
5 February CAHSEE results available – DO
10 Import 8th grade immunizations
11 P2 ADA Report Due – DO
15 MAA File - DO
16 CALPADS Uploads - DO
20 Run Attendance Audit Report – Site
20 Complete pre-registration for 2012-13 scheduling (all feeder schools and on-site students)
- Site
20 Ninth ADA month ends ***due to DO 4-25, 4 p.m. - Site***
20 Fourth quarter deficiency notices, comprehensive schools – Site
20 Fifth Session report cards, alternative ed – site
24-26 STAR Testing – Site
30 Enrollment Numbers - DO

MAY 2012
(May 14 - July 18 - CALPADS Course Comp Program Participation - Discipline/Truancy)
CAHSEE Waiver Submission Windows
Anomaly Resolution – Ongoing – DO
Master Scheduling begins for 12-13
3 Classified evaluations due – Site
4 Identify ELC juniors and get permission slips - Site
8-9 CAHSEE Testing – Site
9 CALPADS Uploads – DO
11 Preliminary Master Schedule to DO – Site
14 EOY 1, EOY 2, EOY 3, EOY 4 Official Submission Window
18 Run Attendance Audit Report – Site
18 Tenth ADA month ends ***due to DO 5-25, 4 p.m. – Site***
23 CALPADS Uploads – DO
30 Exit seniors from Plus schools and enroll in comprehensive sites for graduation – Site
31 Enrollment Numbers - DO

JUNE 2012

Anomaly Resolution – Ongoing – DO
1 Send EOY 1, EOY 2, EOY 3 and EOY 4 reports to sites and district for review
4 Second semester report cards, comprehensive schools - Site
4 Run Attendance Audit Report – Site
4 Sixth session report cards, alternative ed; final ADA report – Site
8 Summer School Starts
11 Computer - Advanced Math Proficiencies process - DO
18 Start calling students who have not picked up packets - Site
28 Deadline for students to pick up pre-registration packets – Site
28 Report to DO on status/disposition of students not picking up packets/responding to calls
- Site
28 Drop all students who have not picked up pre-registration packets – Site

JULY 2012

Anomaly Resolution – Ongoing - DO
Enter/update all pertinent student data – Site
Run Query – Missing Pre-Id Data
1. End of Course Exam Results posted in Datawise – DO
12 New year rollover – DO
18 Certification Deadline for EOY 1, EOY 2, EOY 3, EOY 4

AUGUST 2012

(Aug. 1 - Sept. 1 - CALPADS AYP/API)

Anomaly Resolution – Ongoing – DO
6 Finalize Master Schedule - Site
13-14 Count of locator cards not picked up – Site
14 Drop all no-shows by end of day – Site
17 Run Attendance Audit Report - Site
17 Finish entering any missing student data - Site
Run Query – Missing Pre-Id Data
20 Request SSIDs for new students - DO
22 October CAHSEE Pre-ID file due – DO
24 Run Enrollment Audit Listing and Students Actively Enrolled in Two Schools reports; send to schools to resolve problems - DO
31 Enrollment Numbers - DO

Appendix C
Sample Job Description #1
Application Support Specialist

Position Summary:

Under general supervision of the Manager of Information and Technology, will support users in the use of Student Information System (SIS) software and other district resource application systems. Will provide technical support for site personnel, training, software updates, trouble-shooting, and other PC/MAC applications as necessary.

Representative Duties:

1. Manage and maintain daily tasks for student information systems and district resource application systems.
2. Support site personnel in the use and proper procedures of student information systems and district resource application systems.
3. Support internal personnel within the Information and Technology Department and oversee system protocols that directly affect the operation and functions of district systems.
4. Complete CALPADS Fall and Spring data submissions.
5. Provide training for all Student Information Systems software and CALPADS.
6. Provide technical support to site users and district system users.
7. Install and maintain Student Information System components district wide, such as, but not limited to: PowerSchool, DataDirector, Email, CALPADS, Fiscal 2000, NutriKids, and district web site.
8. Develop district procedures, and system protocols to support department administration and site functions.
9. Assist in the support of systems and projects as directed by Manager of Information and Technology.
10. Coordinate SIS new year rollover and printing of required district reports.
11. Manage productivity in the area of new student information technology and provide the Information Technology department and district with recommendations regarding the district's student information systems.
12. Be accountable for integrity of district information system data.
13. Responsible for the preparation of files for electronic transmission of data to various state and education agencies.

14. Download and import testing results and other data from CALPADS, and or DataDirector, Power School SIS
15. system into testing services.
16. Complete all necessary Erate filing 470, 471, and Item 21 for successful SLD posting.
17. Perform related duties as assigned.

Qualifications:

Knowledge of:

1. 5-8 years of directly related experience in the student information field.
2. Demonstrates competence in Windows operating system environment.
3. Knowledge and 3-5 years experience with Windows XP, Windows 7.
4. Expert knowledge of Excel and data manipulation.
5. Knowledge and experience with CALPADS, PowerSchool, DataDirector, Web development
6. Possess current industry knowledge of student database system procedures.
7. Possess communication skills to convey technical knowledge in a clear manner. Demonstrate the ability to assist in resolving various software issues that arise.
8. Knowledge in the areas of training and instructional programs to improve staff knowledge and the effective use of student information systems and other various software systems.

Ability to:

1. Work within and contribute as an integral part of the Information Technology team; systematic thinker.
2. Ability to work with different file formats for import and export.
3. Communicate and work effectively with others.
4. Understand written and oral instructions.
5. Organize and plan an effective work schedule with users.
6. Install and maintain complex database systems, and applications.
7. Analyze and debug database applications and software problems.
8. Train others in the use and functions of database systems.
9. Provide and maintain documentation of installed systems.

10. Work unsupervised on complex software problems.
11. Communicate and work with vendors to diagnose and eliminate software problems.
12. Respects and maintains professional confidences with all district employees.
13. Utilizes appropriate professional channels for communicating personal/ professional concerns.
14. Demonstrates effective project management and end-user management skills.
15. Work and recognize the necessity for accurate and precise attention to details.
16. Prepare flow and logic diagrams.
17. Develop costs and analyze data for district reports.
18. Work overtime when needed or as directed by the Director of Information and Technology.
19. Be able to work around students, staff, parents, and administration.

Education and Experience

1. 5-8 years of experience with student information systems and technology background.
2. Specialized student information software training.
3. CALPADS experience.

Environment:

1. Office environment
2. Constant interruptions
3. High production environment

Physical Demands:

1. Dexterity of hands and fingers to operate a computer keyboard and other required office machinery.
2. Occasionally lift, carry, push, pull, or otherwise move objects weighing 20 to 40 pounds of force
3. Sitting for extended periods of time.

4. Hearing and speaking to exchange information in person and on the telephone.
5. Can travel in district and/or personal motor vehicle.

License and Certificates

1. Valid California Driver's License.
2. Personal transportation needed for job-related district travel.
3. Obtain auto liability insurance.

Sample Job Description #2
Manager Information Technology

Position Summary:

Under minimal supervision, will coordinate with the users in the purchase, installation and support of networking and desktop hardware and software. Will manage and supervise the tech support staff as needed. Will provide hands-on technical support for LAN/WAN connectivity, email, network trouble-shooting, servers, VoIP phone systems and other PC/MAC applications. The fundamental objectives of this position is to ensure that the district and its various agencies, schools and sites, students, parents, and community, as well as state and government agencies are provided with consistent and reliable access to the district's technology resources.

Essential Functions:

Example of Duties:

1. Manage and maintain daily tasks for IT department staff.
2. Assign and schedule technicians for district technology projects.
3. Assist users in selecting appropriate desktop and network hardware and software.
4. Provide technical support for network, phone system, and video.
5. Install and maintain local and wide area network components, such as, Windows Server 2008R2, Cisco routers, Cisco switches, Cat 6 cabling, fiber optics.
6. Develop automated procedures through staff in support of departmental functions.
7. Assist in the support of systems as directed by direct supervisor.
8. Maintain web content filters.

Qualifications:

Training and Experience:

1. 5-7 years of experience installing and maintaining networks.
2. Bachelor's degree and/or extensive equivalent training and experience.
3. Extensive equivalent training and experience may be substituted for bachelor's degree.
4. Certified Microsoft courses preferred.
5. Certified Cisco Network Administrator (CCNA) is highly preferred.
6. A+ Certification required, or equivalent experience.

Knowledge Of:

1. Macintosh and PC systems, i.e., Windows XP, Windows 7
2. Network operating systems, i.e., Windows 2008, Cisco IOS 11x-12.
3. Office suite applications MS Office XP and 2010.
4. Good knowledge of email systems.
5. iPad deployment.
6. Cisco VoIP phone systems
7. Use of networking and desktop hardware components.
8. Knowledge of LAN and WAN network protocols, IP, OSPF, BGP, IPv6
9. Good working knowledge of Cisco routers and IOS configurations.
10. IIS web server configurations and setup.
11. Excellent working knowledge of Microsoft Active Directory, GPOs
12. Good scripting knowledge, VBS, Pearl, PHP
13. Working knowledge of VoIP, convergence technologies.
14. Wireless networks.
15. Knowledge of Cisco ASA firewalls.

Ability To:

1. Work within and lead a team.
2. Be a leader and communicate and work effectively with others.
3. Understand written and oral instructions.
4. Organize and plan an effective work schedule with users.
5. Install personal computers, networks, and applications.
6. Diagnose and fix hardware and software problems, both in person and remotely.
7. Train others in the use and functions of network resources.
8. Provide and maintain documentation of installed systems.
9. Provide excellent customer service.
10. Work at multiple sites and locations each day.

Licenses and Other Requirements:

1. Valid California Driver's License

Physical Demands:

1. The physical requirements indicated below are examples of the physical aspects that this position classification must perform in carrying out essential job functions.
2. Persons performing service in this position classification-will exert 0 to 50 pounds of force occasionally to lift, carry, push, pull, or otherwise move objects.
3. May occasionally lift and stack heavy objects not to exceed 50 lbs.
4. This type of work involves sitting most of the time, but may involve walking or standing for brief periods.
5. Perceiving the nature of sound, near and far vision, depth perception, providing oral information, the manual dexterity to operate business related equipment, and handle and work with various materials and objects are important aspects of this job.
6. Dexterity of hands and fingers to operate a computer keyboard
7. Bending at the waist, kneeling or crouching to file materials
8. Reaching overhead, above the shoulders and horizontally to retrieve files

Appendix D
Sample Configuration

The configuration below assumes that the switch is loaded with a K9 image to support encryption. This is a sample configuration

Enable timestamps on log output that includes the data and time down to the millisecond.
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime

Disable source routed packets.
no ip source-route

Enable locally stored passwords to be encrypted.
service password-encryption

Define hostname to be used by the local system.
hostname Site-devicemodel-location (RES-3560G-IDF1)

Define Enable Secret passwords
enable secret 5 XXXXXXXXXXX

Define local user account. This account will be test for local login before RADIUS. This account should be unique to the site and only given on a need to know basis. Day to day management authentication to be provided by RADIUS.
username <site admin name> privilege 15 password 7 XXXXXXXXXXX

Define a RADIUS server group that includes the available servers and ports. Define an authentication banner warning of unauthorized usage. Define authentication to first check the local database and then use RADIUS if the account is not found. Use common session IDs.
aaa new-model
aaa group server radius BSD-<site name>
server <radius server ip> auth-port 1645 acct-port 1646
server <radius server ip> auth-port 1645 acct-port 1646
aaa authentication banner ^CUnauthorized use is prohibited.^C
aaa authentication fail-message ^CFailed login^C
aaa authentication login default local group BSD-<site name>
aaa session-id common

Define time zone data for syslog output and local logging.
clock time zone PT -8
clock summer-time PT recurring

Define domain name used for generating local RSA keys.

ip domain name <domain name>

Generate local RSA general use keys to enable SSH. When prompted accept the modulus of 512.
crypto key generate rsa general-keys

Define SSH session timeout and retry values.
ip ssh time-out 60
ip ssh authentication-retries 2

Define spanning tree mode of operation. Define spanning tree priorities on each VLAN using the following values:
Tier 1 switch: 4096
Tier 2 switch: 8192
Tier 3 switch: 12288
Tier 4 switch: implied default of 32768
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority <defined tier value>
spanning-tree vlan 135 priority <defined tier value>
spanning-tree vlan 935 priority <defined tier value>

Typical end node interface. The port is put into access mode in the appropriate VLAN and instructed to not to negotiate any other mode. Portfast is enabled to allow for fast convergence for end stations. BPDUguard is enabled in case someone connects a switch to the port and potentially cases spanning tree to re-converge. CDP is disabled.
interface FastEthernet0/1
 description <describe connected end node>
 switchport access vlan XXX
 switchport mode access
 switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpduguard enable
  no cdp enable

Typical unused port deployed where ports are not anticipated to be used. No port should be left in the default VLAN 1 unless there is a specific reason. The port is put into access mode in the DEAD VLAN (TBD) and instructed to not to negotiate any other mode. Portfast is enabled to allow for fast convergence for end stations. BPDUguard is enabled in case someone connects a switch to the port and potentially cases spanning tree to re-converge. CDP is disabled.
interface FastEthernet0/1
 description UNUSED PORT
 switchport access vlan XXX
 switchport mode access

```
  switchport nonegotiate
        spanning-tree portfast
       spanning-tree bpduguard enable
       no cdp enable
```

Typical trunking interface. The trunk encapsulation mode is manually defined (not needed on all switches as dot1q is default on some platforms) and the port is put into trunking mode. The allowed VLANs on the trunk are manually defined. CDP is disabled.

```
interface GigabitEthernet0/1
  description <describe connected end node>
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport trunk allowed vlans X,Y,Z
  no cdp enable
```

Define and describe VLAN 1 management/potential L3 interface. Disable route caching. Disable IP redirects. Disable IP unreachable packets. Disable IP proxy ARP (may cause an issue on some systems).

```
interface Vlan1
  description <description of VLAN 1>
        ip address <ip address of device>
        no ip route-cache
       no ip redirects
        no ip unreachables
        no ip proxy-arp
```

Define other VLANs if the switch is multi-layer. Disable route caching. Disable IP redirects. Disable IP unreachable packets. Disable IP proxy ARP (may cause an issue on some systems).

```
interface VlanX
  description <description of VLAN X>
        ip address <ip address of device in VLAN X>
        no ip route-cache
       no ip redirects
        no ip unreachables
        no ip proxy-arp
```

Define default route.

```
ip default-gateway <default route>
```

Disable web management systems unless absolutely needed. If needed define access control lists that restrict access to trusted systems that are authorized.

```
no ip http server
no ip http secure-server
```

Access lists to define ranges and hosts to accept SNMP read only and read write communication from.
access-list 20 permit <SNMP RO range> 0.0.0.255
access-list 20 permit host <SNMP RO host>
access-list 20 deny any log
access-list 30 permit <SNMP RW range> 0.0.0.255
access-list 30 permit host <SNMP RW host>
access-list 30 deny any log

Define SNMP logging level as well as target log server. Define a logging facility that is used by this device type (EX: switches = local3, routers = local4, access points = local5 and firewalls = local6). Most log servers maintain a separate log file for each facility; this can speed up searching for specific log entries when the device type is known. Define SNMP read only community credentials as well as systems trusted to query this data via access-list 20. Define SNMP read write community credentials as well as systems trusted to query and set this data via access-list 30. Define SNMP system description, contact and location.
logging trap critical **(recommend informational)**
logging <log server IP>
logging facility local3
snmp-server community <community ID> RO 20
snmp-server community <community ID> RW 30
snmp-server location <site name>
snmp-server contact <system contact>
snmp-server chassis-id <device description>

Define RADIUS servers, ports and keys used for authentication.
radius-server host <radius host ip> auth-port 1645 acct-port 1646 key 7 XXXXXXXXXX
radius-server host <radius host ip> auth-port 1645 acct-port 1646 key 7 XXXXXXXXXX
radius-server source-ports 1645-1646

Define a login banner in the event an individual that is not authorized logs into the system.
banner motd ^C
--- Warning ---
This is a private computer facility protected by a security system. Access to and use of this facility requires explicit written, current authorization and is strictly limited to the purposes of this organization's business.

Unauthorized or any attempt at unauthorized access, use, copying, alteration, destruction or damage to its data, programs, or equipment may violate the Federal Computer Fraud and Abuse Act of 1986 as well as applicable state law and may result in criminal or civil liability, or both.
^C

Access list to define trusted management ranges and hosts that are permitted remote SSH access to this device.

```
access-list 10 permit <management range> 0.0.0.255
access-list 10 permit host <management host>
access-list 10 deny any log
```

Local console will be controlled by the local database then RADIUS authentication. Remove "transport output xxx" command to deny using this device as a jumping point to the rest of the network. Session timeout in 5 minutes.

```
line con 0
  password 7 XXXXXXXXXXX
  exec-timeout 5 0
        logging synchronous
```

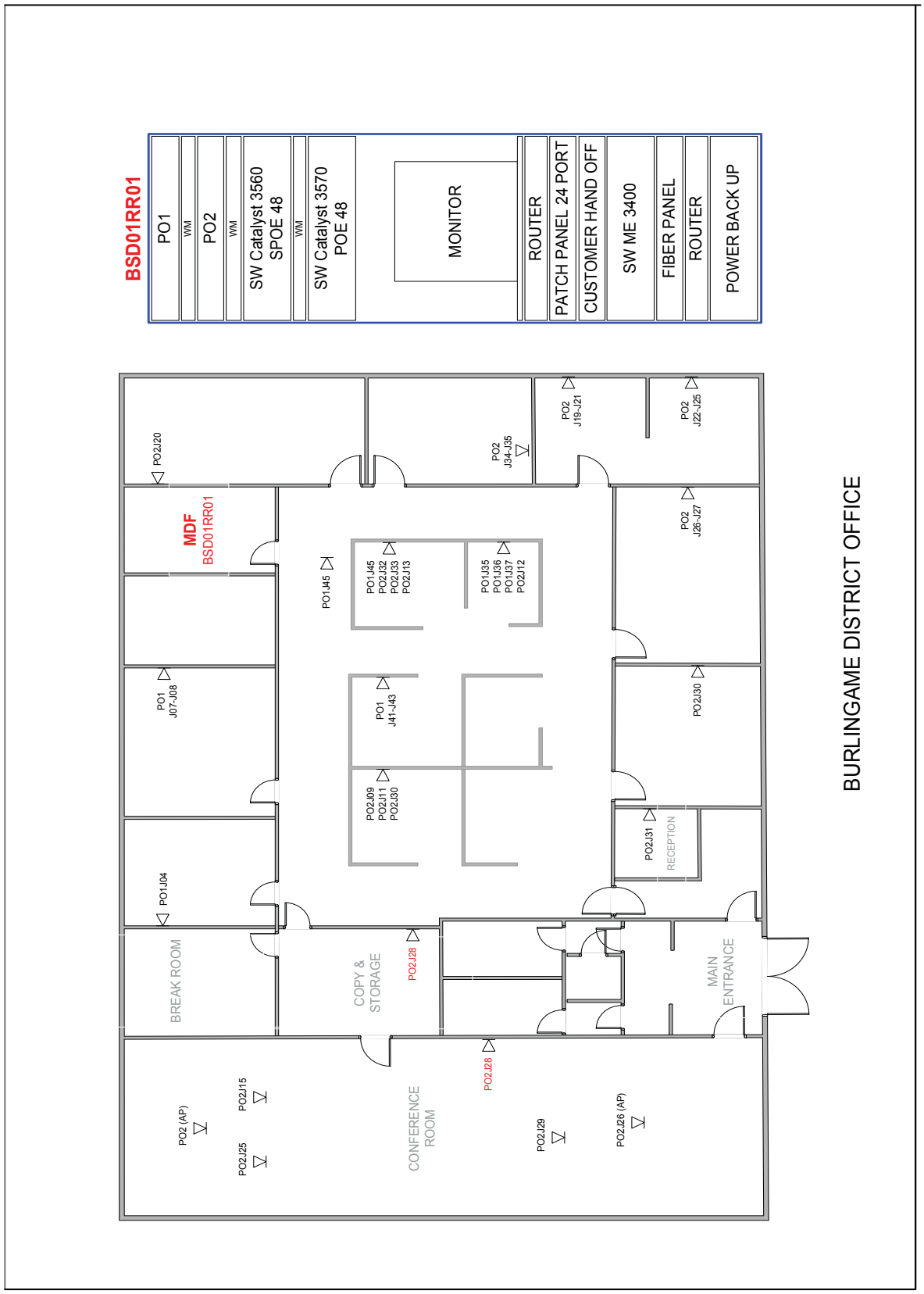
Local VTY ports will be controlled by local database then RADIUS authentication. Only SSH is permitted for login and only from systems specified in access-list 10. Session timeout in 5 minutes.

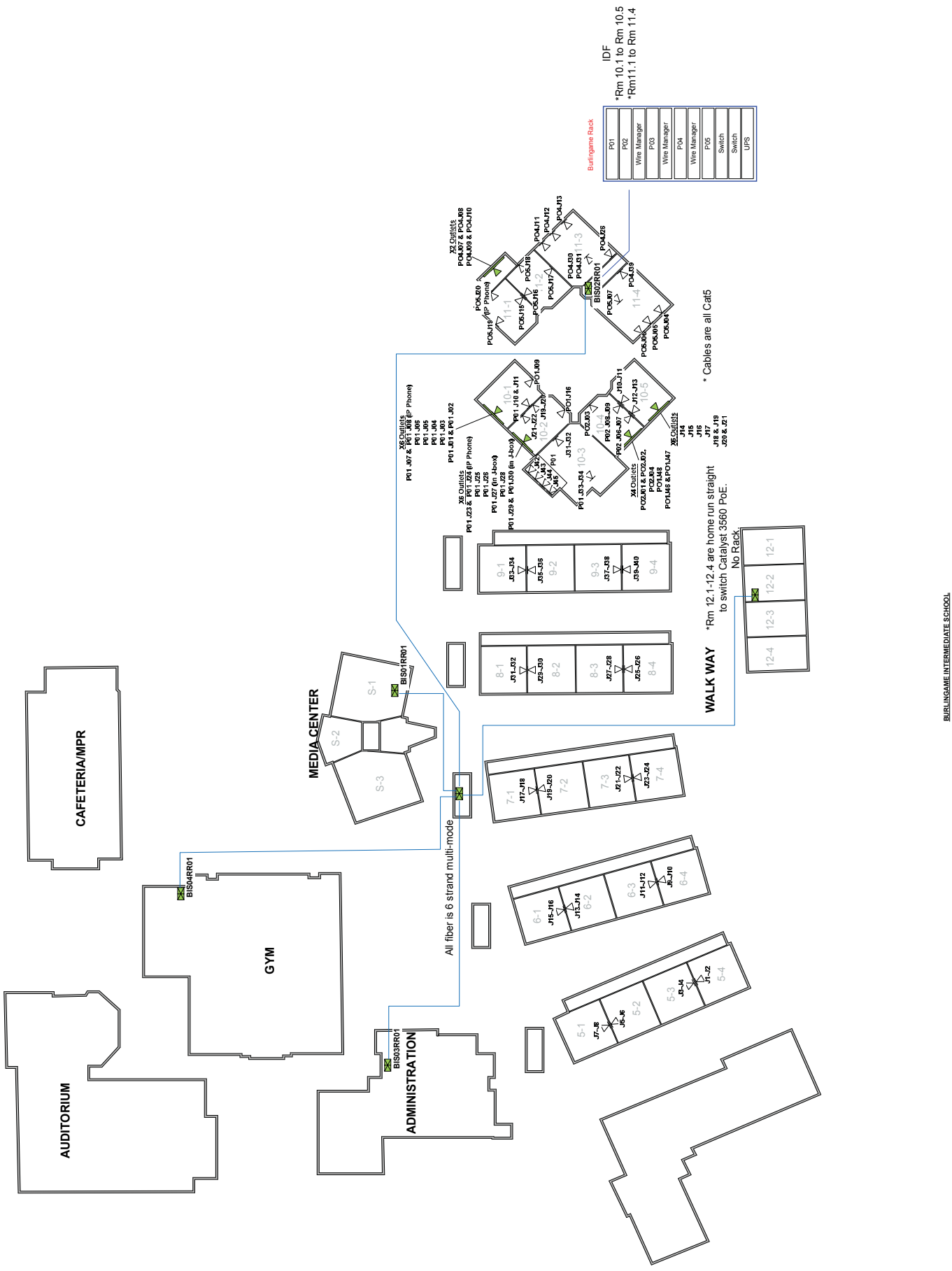
```
line vty 0 4
  password 7 XXXXXXXXXXX
         transport input ssh
        exec-timeout 5 0
        access-class 10 in
        logging synchronous
line vty 5 15
         password 7 XXXXXXXXXXX
         transport input ssh
        exec-timeout 5 0
        access-class 10 in
        logging synchronous
```

Define NTP server to synchronize local clock to, syslog output will use this clock to timestamp output.

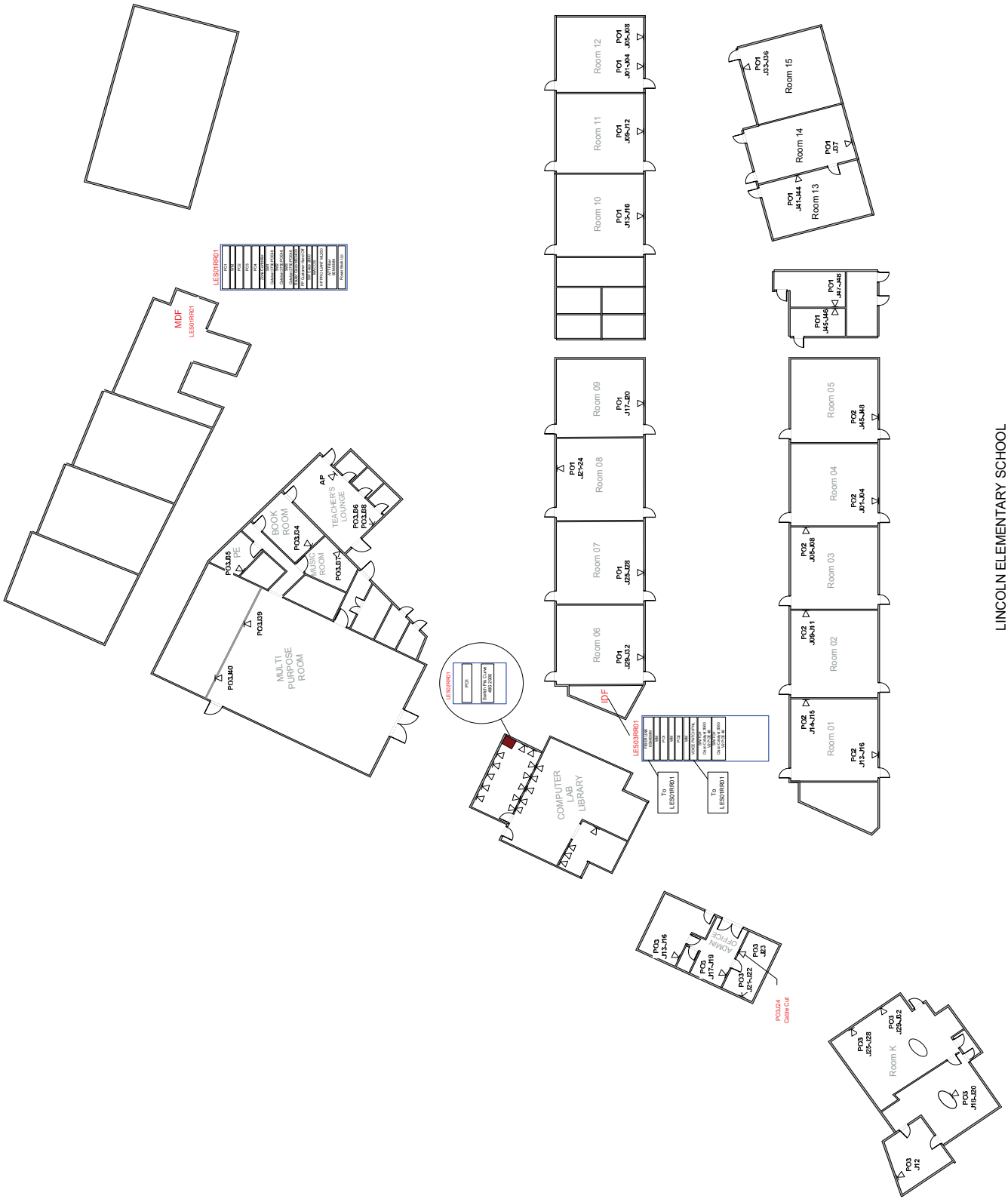
```
ntp server <NTP server IP>
```

Appendix E
Advanced Data Communications - Network Mapping Diagrams

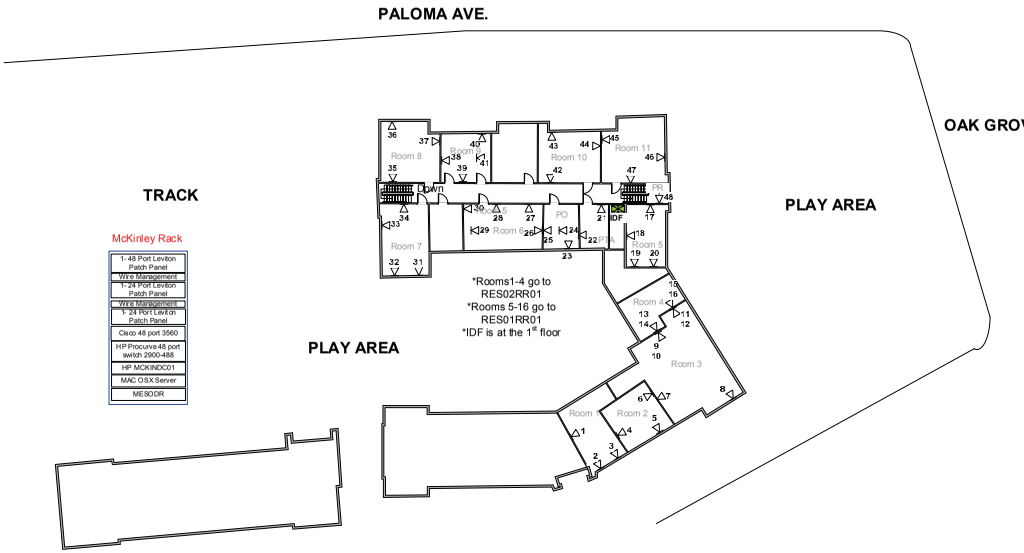


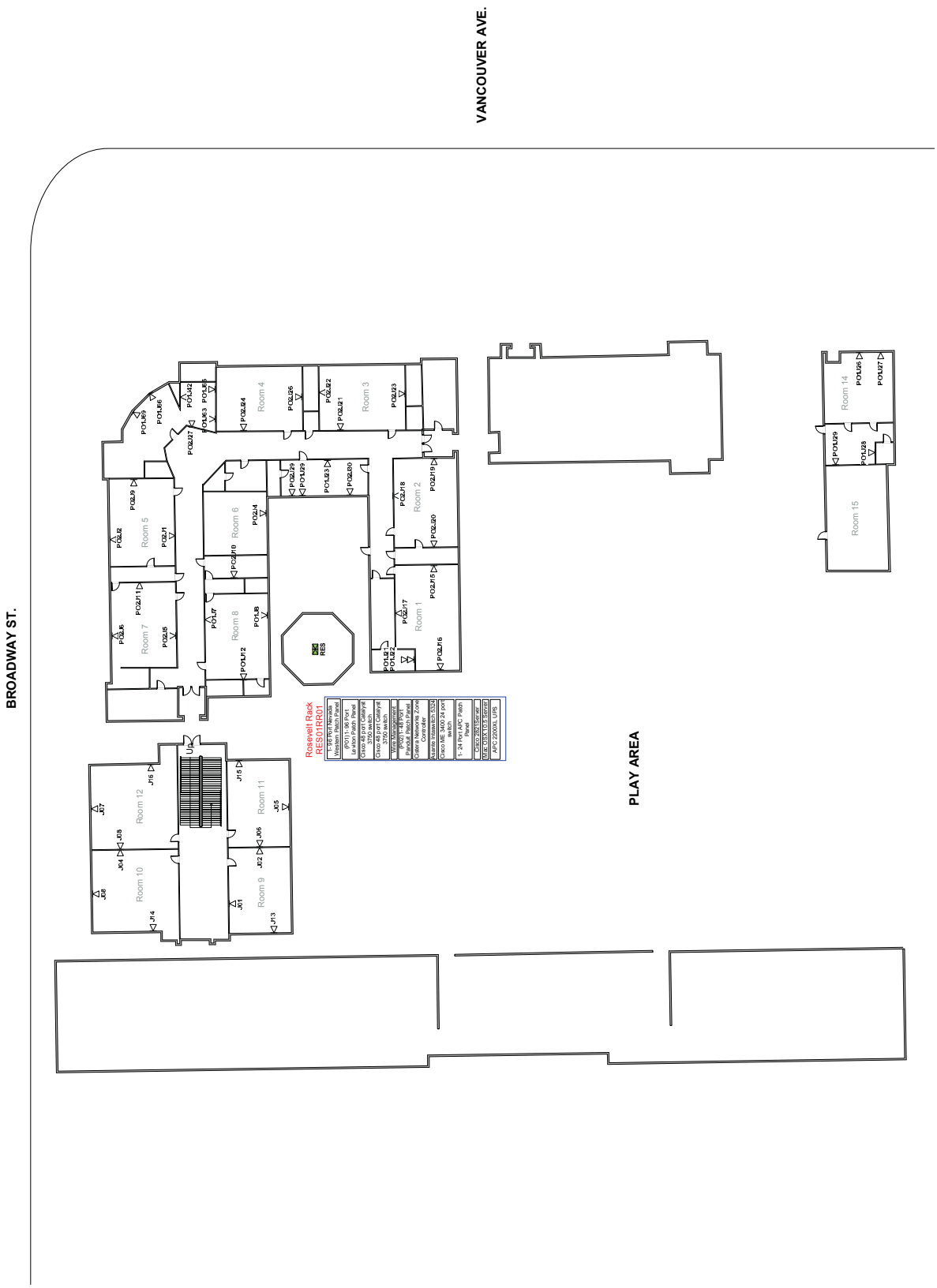

IDF
*Rm 10.1 to Rm 10.5
*Rm11.1 to Rm 11.4
Burlingame Rack
P01
P02
Wire Manager
P03
Wire Manager
P04
Wire Manager
P05
Switch
Switch
UPS
* Cables are all Cat5
*Rm 12.1-12.4 are home run straight to switch Catalyst 3560 PoE.
No Rack.
WALK WAY
MEDIA CENTER
CAFETERIA/MPR
GYM
AUDITORIUM
ADMINISTRATION
All fiber is 6 strand multi-mode
BIS01RR01
BIS02RR01
BIS03RR01
BIS04RR01
BURLINGAME INTERMEDIATE SCHOOL

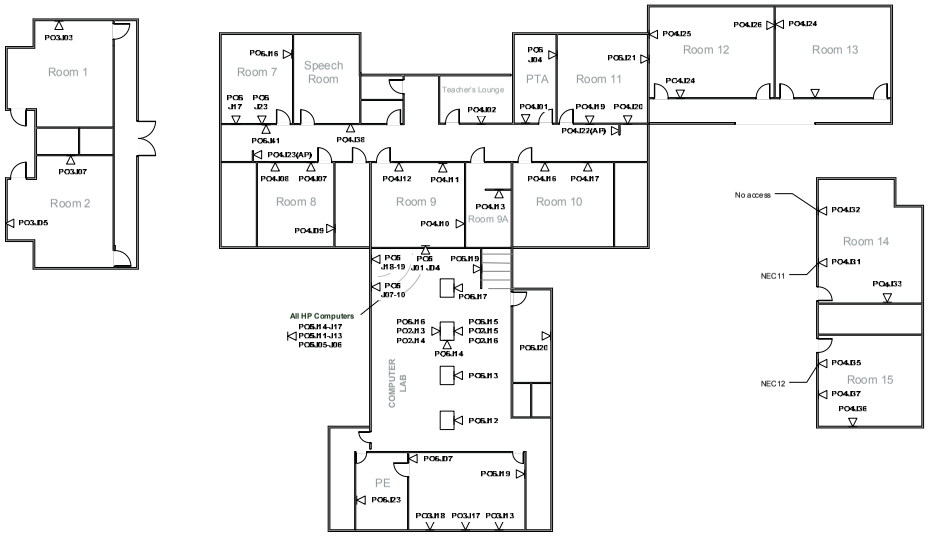
FRANKLIN ELEMENTARY SCHOOL

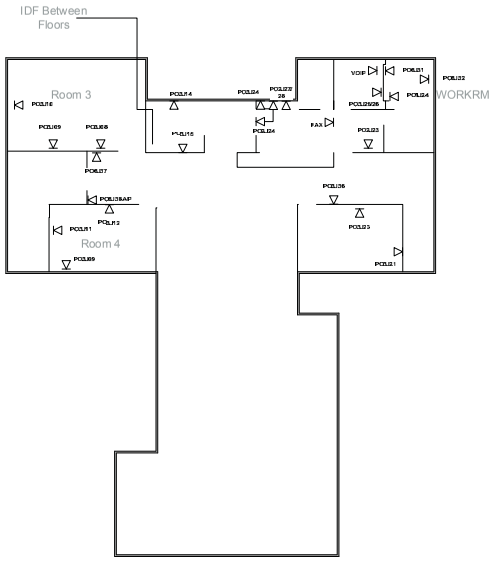

LINCOLN ELEMENTARY SCHOOL
MDF
LES01RR01
MULTI PURPOSE ROOM
PE
BOOK ROOM
TEACHERS LOUNGE
AP
COMPUTER LAB LIBRARY
ADMIN OFFICE
Room 01
Room 02
Room 03
Room 04
Room 05
Room 06
Room 07
Room 08
Room 09
Room 10
Room 11
Room 12
Room 13
Room 14
Room 15
Room K
LES02RR01
LES03RR01
To LES01RR01
To LES01RR01
PO3J24 Cable Cut

1ST FLOOR

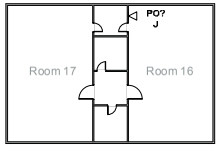

PALOMA AVE.
OAK GROVE AVE.
TRACK
PLAY AREA
PLAY AREA
McKinley Rack
1- 48 Port Leviton Patch Panel
Wire Management
1- 24 Port Leviton Patch Panel
Wire Management
1- 24 Port Leviton Patch Panel
Cisco 48 port 3560
HP Procurve 48 port switch 2900-48S
HP MCKINDC01
MAC OSX Server
MESODR
*Rooms1-4 go to RES02RR01
*Rooms 5-16 go to RES01RR01
*IDF is at the 1st floor
Room 8
Room 10
Room 11
Room 7
Room 6
Room 4
Room 3
Room 2
Room
Room 9
Room 5
Room
Room
Room


VANCOUVER AVE.
BROADWAY ST.
ROSEVELT ELEMENTARY SCHOOL
PLAY AREA
Room 1
Room 2
Room 3
Room 4
Room 5
Room 6
Room 7
Room 8
Room 9
Room 10
Room 11
Room 12
Room 14
Room 15
Rosevelt Rack
RES01RR01

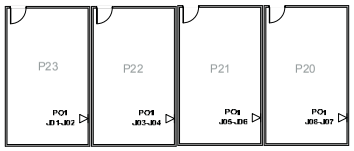




Second Floor



PORTABLES



WASHINGTON ELEMENTARY SCHOOL

Appendix F
Advanced Data Communications Network Label Inventories

Burlingame School District
Network Discovery Audit

SITE	**Burlingame DO**	**RACK**	**BSD01RR01**
		PATCH PANEL	**P01**

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001				N/A
J002				N/A
J003				N/A
J004	2	Office	phone	no acess
J005				N/A
J006				N/A
J007	2	Asst .Supervisor	phone	
J008		Asst .Supervisor	computer	not used
J009				N/A
J010				N/A
J011				N/A
J012				N/A
J013				N/A
J014				N/A
J015				N/A
J016				N/A
J017				N/A
J018				N/A
J019	2	Office	phone	
J020		Office	computer	
J021	2	Office	phone	
J022	2	Office	computer	
J023		Office	computer	
J024	2	Office	phone	
J025	1	Office	phone	
J026		Office	computer	
J027	2	Office	phone	
J028				N/A
J029	2	Office	phone	
J030	2	Office	computer	
J031		Office	computer	no access
J032				N/A
J033	2	Office	phone	no access
J034				N/A
J035	2	Cubicle	phone	
J036	2	Cubicle	phone	
J037	2	Cubicle	phone	
J038				N/A
J039				N/A
J040	1	Cubicle	phone	
J041	2	Cubicle	phone	
J042	2	Cubicle	computer	
J043		Cubicle	Fax	analog
J044				N/A
J045	2	Cubicle	computer	
J046				N/A
J047				N/A
J048				N/A

Note: N/A = Not found

Franklin

SITE	Burlingame DFO	RACK	BSD01RR01
		PATCH PANEL	P02

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001				N/A
J002		Cubicle		Not Used
J003				N/A
J004				N/A
J005				N/A
J006				N/A
J007	1	Cubicle	Phone	
J008				N/A
J009		Cubicle		Not Used
J010	1	Cubicle		Not Used
J011		Cubicle		Not Used
J012	2	Cubicle	Phone	
J013	2	Cubicle	computer	
J014				N/A
J015	2	Board rm	Phone	
J016				N/A
J017	2	Board rm	A.P.	
J018	2	Supervisor	Phone	No Acess
J019	2	Copier		
J020	2	Supervisor		
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025	1	Board rm	Phone	
J026	2	Board rm	computer	
J027	2	Board rm		Not Used
J028	2	Board rm		Not Used
J029		Board rm		Not Used
J030		Board rm		Not Used
J031	1	Receptionist		No Acess
J032	1	Cubicle	Phone	
J033				N/A
J034	1	Office	Phone	
J035	1	Office	computer	
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Burlingame School District
Network Discovery Audit

SITE	**BURLINGAME IS**	**RACK**	**BIS01RR01**
		PATCH PANEL	**P01**

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	5.4	Phone	
J002	1	5.4	Computer	
J003	1	5.3	Computer	
J004	1	5.3	Phone	
J005	1	5.2	Computer	
J006	1	5.2	Phone	
J007	1	5.1	Computer	
J008	2	5.1	Phone	
J009	2	6.4	Phone	
J010	2	6.4	Computer	
J011	2	6.3	PHONE	
J012	2	6.3	Computer	
J013	1	6.2	Computer	
J014	1	6.2	Phone	
J015	1	6.1	Computer	
J016	2	6.1	Phone	
J017	2	7.1	Phone	
J018	2	7.1	Computer	
J019	1	7.2	Phone	
J020	1	7.2	Computer	
J021	1	7.3	Phone	
J022	1	7.3	Computer	
J023	2	7.4	Computer	
J024	2	7.4	Phone	
J025	2	8.4	Computer	
J026	1	8.4	Phone	
J027	1	8.3	Phone	
J028	1	8.3	Computer	
J029	1	8.2	Phone	
J030	2	8.2	Computer	
J031	2	8.1	Phone	
J032	1	8.1	Computer	
J033	2	9.1	Phone	
J034	1	9.1	Computer	
J035	1	9.2	Phone	
J036	1	9.2	Computer	
J037	1	9.3	Phone	
J038	1	9.3	Computer	
J039	2	9.4	Phone	
J040	1	9.4	Computer	
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Franklin

SITE	**BURLINGAME INTER. School**	**RACK**	**BIS02RR01**
		PATCH PANEL	**P01**

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	10.1	COMPUTER	
J002		10.1		Not Used
J003		10.1		Not Used
J004		10.1		Not Used
J005		10.1		Not Used
J006				N/A
J007		10.1		Not Used
J008		10.1		Not Used
J009		10.1		Not Used
J010		10.1		Not Used
J011	1	10.1	PHONE	
J012		10.1		Not Used
J013				N/A
J014				N/A
J015				N/A
J016		10.2		Not Used
J017				N/A
J018				N/A
J019		10.2		Not Used
J020		10.2		Not Used
J021		10.2		Not Used
J022		10.2		Not Used
J023				N/A
J024	1	10.2	PHONE	
J025		10.2		Not Used
J026		10.2		Not Used
J027		10.2		Not Used
J028	1	10.2	COMPUTER	
J029		10.2		Not Used
J030		10.2		Not Used
J031	1	10.3	PHONE	
J032	1	10.3	COMPUTER	
J033		10.3		Not Used
J034	1	10.3	COMPUTER	
J035		10.3		Not Used
J036		10.3		Not Used
J037	1	10.3		Not Used
J038	1	10.3		Not Used
J039		10.3		Not Used
J040		10.3		Not Used
J041		10.3		Not Used
J042		10.3		Not Used
J043	1	10.4	PHONE	
J044		10.4		Not Used
J045		10.4		Not Used
J046	1	10.4	COMPUTER	
J047		10.4		Not Used
J048		10.4		Not Used

SITE	BURLINGAME IS	RACK	BIS02RR01
		PATCH PANEL	P02

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001		10.4		Not Used
J002		10.4		Not Used
J003		10.4		Not Used
J004	1	10.4	PHONE	
J005				N/A
J006		10.4		Not Used
J007		10.4		Not Used
J008		10.4		Not Used
J009		10.4		Not Used
J010		10.5		Not Used
J011		10.5		Not Used
J012		10.5		Not Used
J013		10.5		Not Used
J014	1	10.5	PHONE	
J015	1	10.5	Computer	
J016		10.5		Not Used
J017		10.5		Not Used
J018		10.5		Not Used
J019		10.5		Not Used
J020		10.5		Not Used
J021		10.5		Not Used
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Burlingame School District
Network Discovery Audit

SITE	**Franklin ES**	**RACK**	**FES01RR01**
		PATCH PANEL	**P01**

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	2	RM.1	Phone	
J002	2	RM.1	Computer	
J003	2	RM.1		Not Used
J004	2	RM.1		Not Used
J005	2	RM.2	Phone	
J006	2	RM.2	Computer	
J007	2	RM.2		Not Used
J008	2	RM.2		Not Used
J009	2	RM.3	Computer	
J010	2	RM.3	Phone	
J011	2	RM.3		Not Used
J012	2	RM.3		Not Used
J013	2	RM.4	Computer	
J014	2	RM.4	Phone	
J015	2	RM.4		Not Used
J016	2	RM.4		Not Used
J017	2	RM.5		Not Used
J018	1	RM.5	Computer	
J019	1	RM.5		Not Used
J020	1	RM.5		Not Used
J021	1	RM.6	Phone	
J022	1	RM.6	Computer	
J023	1	RM.6		Not Used
J024	1	RM.6		Not Used
J025	1	RM.7	Computer	
J026	1	RM.7	Phone	
J027	1	RM.7		Not Used
J028	1	RM.7		Not Used
J029	1	RM.8		Not Used
J030	1	RM.8	Phone	
J031	1	RM.8	Computer	
J032	1	RM.8		Not Used
J033	1	RM.9	Phone	
J034	1	RM.9	Computer	
J035	1	RM.9		Not Used
J036	1	RM.9		Not Used
J037	1	RM.10	Phone	
J038	2	RM.10	Computer	
J039	2	RM.10		Not Used
J040	2	RM.10		Not Used
J041	2	RM.11		Not Used
J042	2	RM.11		Not Used
J043	2	RM.11	Computer	
J044	2	RM.11	Phone	
J045	2	RM.12		Not Used
J046	2	RM.12	Phone	
J047	2	RM.12	Computer	
J048	2	RM.12		Not Used

Franklin

SITE	Franklin ES	RACK	FES02RR01
		PATCH PANEL	P01

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	29	Wireless	
J002				N/A
J003	1	20	Phone	
J004	1	20	Computer	
J005	1	21		Not Used
J006				N/A
J007	1	21	Computer	
J008	1	21	Phone	
J009	1	22	Wireless	
J010	1	22	Computer	
J011	1	22	Phone	
J012	1	22		NOT USED
J013	1	22		NOT USED
J014				N/A
J015				N/A
J016				N/A
J017				N/A
J018				N/A
J019				N/A
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

SITE	Franklin ES	RACK	FES01RR01
		PATCH PANEL	P02

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	2	RM.K	Phone	
J002	2	RM.K	Computer	
J003	2	RM.K		Not Used
J004	2	RM.K		Not Used
J005	2	RM.14	Phone	
J006	2	RM.14	Computer	
J007	2	RM.14		Not Used
J008	2	RM.14		Not Used
J009	2	RM.15	Computer	
J010	2	RM.15	Phone	
J011	2	RM.15		Not Used
J012	2	RM.15		Not Used
J013	2	RM.16	Computer	
J014	2	RM.16	Phone	
J015	2	RM.16		Not Used
J016	2	RM.16		Not Used
J017	2	RM.17		Not Used
J018	1	RM.17	Computer	
J019	1	RM.17		Not Used
J020	1	RM.17		Not Used
J021	1	RM.18	Phone	
J022	1	RM.18	Computer	
J023	1	RM.18		Not Used
J024	1	RM.18		Not Used
J025	1	RM.19	Computer	
J026	1	RM.19	Phone	
J027	1	RM.19		Not Used
J028	1	RM.19		Not Used
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

SITE	Franklin ES	RACK	FES01RR01
		PATCH PANEL	P03

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	3	Comp lab/library	computer	
J002	3	Comp lab/library	computer	
J003	3	Comp lab/library	computer	
J004	3	Comp lab/library	computer	
J005	3	Comp lab/library	computer	
J006	3	Comp lab/library	computer	
J007	3	Comp lab/library	computer	
J008	3	Comp lab/library	computer	
J009	3	Comp lab/library	computer	
J010	3	Comp lab/library	computer	
J011	3	Comp lab/library	computer	
J012	3	Comp lab/library	computer	
J013	3	Comp lab/library	computer	
J014	3	Comp lab/library	computer	
J015	3	Comp lab/library	computer	
J016	3	Comp lab/library	computer	
J017	3	Comp lab/library	computer	
J018	3	Comp lab/library	computer	
J019				N/A
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

SITE	Franklin ES

RACK	FES01RR01
PATCH PANEL	P04

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	3	Comp lab/library	computer	
J002	3	Comp lab/library	computer	
J003	3	Comp lab/library	computer	
J004	3	Comp lab/library	computer	
J005	3	Comp lab/library	computer	
J006	3	Comp lab/library	computer	
J007	3	Comp lab/library	computer	
J008	3	Comp lab/library	computer	
J009	3	Comp lab/library	computer	
J010	3	Comp lab/library	computer	
J011	3	Comp lab/library	computer	
J012	3	Comp lab/library	computer	
J013	3	Comp lab/library	computer	
J014	3	Comp lab/library	computer	
J015	3	Comp lab/library	computer	
J016	3	Comp lab/library	computer	
J017	3	Comp lab/library	computer	
J018				N/A
J019				N/A
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

PATCH PANEL	P01

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	Rm.12	Computer	
J002	1	Rm.12	Computer	
J003	1	Rm.12	Computer	
J004	3	Rm.12	Phone	
J005	1	Rm.12	Printer	
J006	1	Rm.12		Not Used
J007	1	Rm.12		Not Used
J008	1	Rm.12		Not Used
J009	1	Rm.11		Not Used
J010	1	Rm.11	Computer	
J011	1	Rm.11	Computer	
J012	2	Rm.11	Phone	
J013	2	Rm.10	Phone	
J014	1	Rm.10	Computer	
J015	1	Rm.10	Computer	
J016	1	Rm.10		Not Used
J017	2	Rm.09	Phone	
J018	1	Rm.09	Computer	
J019		Rm.09		Not Used
J020	1	Rm.09	Computer	
J021		Rm.08		Not Used
J022	2	Rm.08	Phone	
J023	2	Rm.08	Computer	
J024	2	Rm.08	Phone	
J025	1	Rm.07	Computer	
J026	2	Rm.07	Phone	
J027		Rm.07		Not Used
J028	1	Rm.07		Not Used
J029	2	Rm.06	Phone	
J030	1	Rm.06	Computer	
J031		Rm.06		Not Used
J032		Rm.06		Not Used
J033	2	Rm.15	Phone	
J034	1	Rm.15	Computer	
J035	1	Rm.15	Computer	
J036		Rm.15		Not Used/ No Switch
J037	2	Rm. 14	Phone	
J038	1	Rm. 14	Computer	
J039	2	Rm. 14		Not Used
J040	2	Rm. 14		Not Used
J041	2	Rm.13	Phone	
J042	1	Rm.13	Computer	
J043	2	Rm.13		Not Used
J044	2	Rm.13		Not Used
J045	2	Rm.05		Not Used
J046	2	Rm.05	Computer	
J047	2	Rm.05		Not Used
J048	2	Rm.05	Phone	

SITE	Lincoln ES	RACK	LES01RR01
		PATCH PANEL	P02

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	2	Rm 4	Phone	
J002	2	Rm 4		Not Used
J003	3	Rm 4		Not Used
J004	2	Rm 4	Computer	
J005	2	Rm 3		Not Used
J006	2	Rm 3	Phone	
J007				N/A
J008	2	Rm 3	Computer	
J009				N/A
J010	3	Rm 2	Phone	
J011				N/A
J012	3	Rm 2	Phone	
J013	2	Rm 2	Computer	
J014				N/A
J015	1	Rm 1	Phone	
J016	2	Rm 1		Not Used
J017	2	Rm 1	Computer	
J018				
J019				
J020	2	Rm k	Computer	
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027	2	Library	Computer	
J028	2	Library	Computer	
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

SITE	Lincoln ES	RACK	LES01RR01
		PATCH PANEL	P03

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	3	Library	Printer	
J002	2	Library	Computer	
J003	2	Library	Computer	
J004	2	Library	Printer	
J005	2	Library	Phone	
J006	2	Library	Computer	
J007				N/A
J008				N/A
J009				N/A
J010				N/A
J011				N/A
J012	3	RM K	Going to a 66 block	
J013	2	Office	Phone	
J014	1	Office	Phone	
J015	1	Office	Computer	
J016	1	Office	Computer	
J017	2	Office	Phone	
J018				N/A
J019				N/A
J020				N/A
J021	2	Office	Phone	
J022	2	Office	Phone	
J023	3	Office	Phone	
J024				
J025	2	RM K	Phone	Going to 66 block
J026		RM K		Not Used/ No Device/ No Switch
J027		RM K		Not Used/ No Device/ No Switch
J028		RM K		Not Used/ No Device/ No Switch
J029	3	RM K	Computer	
J030	3	RM K	Computer	
J031	3	RM K		Not Used
J032	3	RM K		Not Used
J033	3	Office	Phone	
J034	3	Book rm		Not Used
J035	3	P.E.	Phone	
J036				N/A
J037	2	Music Rm	Phone	
J038				N/A
J039	3	MPR		Not Used
J040	1	MPR		Not Used
J041	1	Faculty	Computer	
J042	1	Faculty	Phone	
J043	2	Faculty	Phone	
J044		Faculty		Not Used / No Switch
J045		Rm B		Not Used / No Switch
J046	2	Rm B	Phone	
J047	2	Rm A	Computer	
J048	1	Rm A	Computer	

Note: N/A = Not Found

SITE	Lincoln ES	RACK	LES01RR01
		PATCH PANEL	P04

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001				N/A
J002				N/A
J003	1	Library	Feed 3	Feeds to LES01RR02
J004	1	Library	Feed 4	Feeds to LES01RR03
J005	1	Library	Feed 5	Feeds to LES01RR04
J006	1	Library	Feed 3	Feeds to LES01RR05
J007	1	Library	Feed 3	Feeds to LES01RR06
J008	1	Library	Feed 3	Feeds to LES01RR07
J009				N/A
J010				N/A
J011				N/A
J012				N/A
J013				N/A
J014				N/A
J015				N/A
J016				N/A
J017				N/A
J018				N/A
J019				N/A
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024	2	Work room	Phone	
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Burlingame School DistrictNetwork Discovery Audit

SITE **MCKINLEY ES**

RACK **MES01RR01**
PATCH PANEL **P01**

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	5		N/A
J002	1	5		N/A
J003	1	5		N/A
J004	1	5		N/A
J005	1	6		N/A
J006	1	6		N/A
J007	1	HALLWAY	COMPUTER	
J008				N/A
J009	1	6		N/A
J010	1	7		N/A
J011	1	7		N/A
J012	1	7		N/A
J013	1	7		N/A
J014	1	8		N/A
J015		8		N/A
J016	1	8		N/A
J017	1	9	WIRELESS	
J018	1	9		N/A
J019	1	9		N/A
J020				N/A
J021	1	10		N/A
J022	1	10		N/A
J023				N/A
J024	1	11		N/A
J025	1	11		N/A
J026	1	11		N/A
J027				N/A
J028	1	13		N/A
J029				N/A
J030	1	15		N/A
J031	1	16		N/A
J032				N/A
J033	1	STUFF ROOM	PHONE	
J034	1	STUFF ROOM	COMPUTER	
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041	1	PSYCHOLOGIST	PHONE	
J042	1	13	WIRELESS	
J043	1	13	PHONE	
J044				N/A
J045	1	BREAK ROOM	PHONE	
J046	1	9	WIRELESS	
J047	1	9	WIRELESS	
J048	1	9	WIRELESS	

Franklin

SITE **MC KINLEY ES**

RACK **MES02RR01**
PATCH PANEL **P01**

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001				N/A
J002				N/A
J003				N/A
J004	2	1	Phone	
J005	2	1		Not Used
J006	2	1	Computer	
J007	2	2	Phone	
J008	2	2	Computer	
J009	2	2		Not Used
J010	2	3	Phone	
J011	2	3		Not Used
J012	2	3	Computer	
J013	2	3		Not Used
J014	2	3		Not Used
J015	2	3		Not Used
J016	2	4	Phone	
J017	2	4	Computer	
J018	2	4		Not Used
J019	2	4		Not Used
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Burlingame School District
Network Discovery Audit

SITE	Roosevelt ES	RACK	RES01RR01
		PATCH PANEL	P02

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001				N/A
J002				N/A
J003				N/A
J004				N/A
J005				N/A
J006				N/A
J007	2	8	Phone	
J008	1	8	Computer	
J009				N/A
J010				N/A
J011				N/A
J012		8		Not uesd
J013				N/A
J014				N/A
J015				N/A
J016				N/A
J017				N/A
J018				N/A
J019				N/A
J020				N/A
J021	1	1	Computer	
J022	2	1	Phone	
J023	1	Principal Off	Computer	
J024	2	Principal Off	Phone	
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042	1	Copy Rm.	Phone	
J043	2	Copy Rm.	Coputer	
J044	1	Copy Rm.		Not used
J045				N/A
J046		Break Rm.	Computer	
J047		Break Rm.	Phone	
J048				N/A

Franklin

SITE	Roosevelt ES

RACK	RES02RR01
PATCH PANEL	PO1

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	2	5	Phone	
J002	1	5	Computer	
J003				N/A
J004				N/A
J005	2	7	Phone	
J006	1	7	Computer	
J007				N/A
J008				N/A
J009	2	5	Phone	
J010				N/A
J011	1	7		Not Used
J012				N/A
J013				N/A
J014				N/A
J015	2	1	Phone	
J016	1	1	Computer	
J017	1	1		Not Used
J018	1	2	Computer	
J019	2	2	Phone	
J020				N/A
J021	1	3	Computer	
J022	2	3	Phone	
J023	1	3		Not Used
J024	2	4	Phone	
J025				N/A
J026	2	4		Not Used
J027	2	Copier Room	Phone	
J028				N/A
J029		OFFICE		N/A
J030		OFFICE		N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

SITE	**WASHINGTON**	**RACK**	**WES01RR01**
	ELEM.	**PATCH PANEL**	**P01**
	School		

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	23	Phone	
J002	1	23	Computer	
J003	1	22	Phone	
J004	1	22	Computer	
J005	1	21	Phone	
J006	1	21	Computer	
J007	1	20	Phone	
J008	1	20	Computer	
J009				N/A
J010				N/A
J011				N/A
J012				N/A
J013				N/A
J014				N/A
J015				N/A
J016				N/A
J017				N/A
J018				N/A
J019				N/A
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024	2	Work room	Phone	
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Note: N/A = Not found

SITE	WASHINGTON ELEM. School	RACK	WES01RR01
		PATCH PANEL	P02

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J002	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J003	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J004	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J005	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J006	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J007	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J008	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J009	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J010	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J011	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J012	4	LIBRARY/ C.LAB	COMPUTER	MAC PC
J013	4	LIBRARY/ C.LAB	COMPUTER	MAC PC
J014	4	LIBRARY/ C.LAB	COMPUTER	MAC PC
J015	4	LIBRARY/ C.LAB	COMPUTER	MAC PC
J016	4	LIBRARY/ C.LAB	COMPUTER	MAC PC
J017	3	MPR	Phone	
J018				N/A
J019				N/A
J020				N/A
J021				N/A
J022				N/A
J023	1	MAIL RM	COMPUTER	
J024	1	OFFICE	COMPUTER	
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Note: N/A = Not Found

SITE	WASHINGTON ELEM.		RACK	WES01RR01
			PATCH PANEL	P03

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	1	3		Not Used
J002				N/A
J003	3	1		Not Used
J004				N/A
J005	1	1	Phone	
J006	2	1	Computer	
J007				N/A
J008				N/A
J009	1	3	Computer	
J010	1	3	Phone	
J011	1	4	Phone	
J012	1	4	Computer	
J013	1	4		Not Used
J014	1	4		Not Used
J015				N/A
J016				N/A
J017				N/A
J018				N/A
J019				N/A
J020	1	5	Phone	
J021	1	5	Computer	
J022				N/A
J023				N/A
J024				N/A
J025	1	Principal	Computer	
J026	3	Principal	Phone	
J027	1	Office	Phone	
J028	3	Office	Computer	
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Note: N/A = Not Found

SITE	WASHINGTON ELEM.	RACK	WES01RR01
		PATCH PANEL	P04

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	4	10A	COMPUTER/HP	HP COMP.
J002	4	STUFF LOUGE	PHONE	CISCO IP
J003	4	OUGE	COMPUTER/HP	HP COMP.
J004	4	10A	COMPUTER/HP	HP COMP.
J005	1	7	COMPUTER	MAC PC
J006	2	7	COMPUTER	MAC PC
J007	4	8	PHONE	CISCO IP
J008	2	8	COMPUTER	MAC PC
J009	2	8		Not Used
J010	1	9	COMPUTER	MAC PC
J011	2	9	PHONE	CISCO IP
J012	4	LIBRARY/ C.LAB	COMPUTER	MAC PC
J013	1	9A	PHONE	CISCO IP
J014	2	9A	COMPUTER	MAC PC
J015	2	9a		Not Used
J016	1	10	PHONE	CISCO IP
J017	2	10	COMPUTER	
J018	2	10		Not Used
J019	1	11	PHONE	CISCO IP
J020	2	11	COMPUTER	MAC PC
J021	2	11		Not Used
J022	1	2nd floor	AP	
J023	2	2nd floor	AP	
J024	1	12	PHONE	CISCO IP
J025	2	12	COMPUTER	MC-PC
J026	2	12		Not Used
J027				N/A
J028	1	13	PHONE	ACKMAC PC
J029	3	13		Not Used
J030	3	13		N/A
J031	14	1	PHONE	CISCO IP
J032				N/A
J033	14	2		Not Used
J034				N/A
J035	15	2	PHONE	CISCO IP
J036	15	2		Not Used
J037	15	2	COMPUTER	MAC PC
J038	3	2nd floor hallway	LINKSYS	4 computers
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Note: N/A = Not Found

SITE	WASHINGTON ELEM.	RACK	WES01RR01
		PATCH PANEL	P05

Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J002	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J003	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J004	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J005	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J006	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J007	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J008	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J009	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J010	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J011	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J012	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J013	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J014	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J015	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J016	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J017	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J018	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J019	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J020				N/A
J021				N/A
J022				N/A
J023				N/A
J024				N/A
J025				N/A
J026				N/A
J027				N/A
J028				N/A
J029				N/A
J030				N/A
J031				N/A
J032				N/A
J033				N/A
J034				N/A
J035				N/A
J036				N/A
J037				N/A
J038				N/A
J039				N/A
J040				N/A
J041				N/A
J042				N/A
J043				N/A
J044				N/A
J045				N/A
J046				N/A
J047				N/A
J048				N/A

Note: N/A = Not Found

SITE	WASHINGTON ELEM.		RACK PATCH PANEL	WES01RR01 P06
Jack Pos	Connected to		DEVICE	Remarks
	SWITCH #	ROOM #		
J001	4	10A	COMPUTER/HP	HP COMP.
J002	2	STUFF LOUGE		NOT USED
J003	4	STUFF LOUGE	COMPUTER	
J004		10A		NOT USED
J005	1	7	COMPUTER	MAC PC
J006	2	7	COMPUTER	MAC PC
J007	4	8	PHONE	CISCO IP
J008	2	8	COMPUTER	MAC PC
J009	2	8		NOT USED
J010	1	9	COMPUTER	MAC PC
J011	4	LIBRARY/ C.LAB	COMPUTER/HP	HP COMP.
J012	1	LIBRARY/ C.LAB	COMPUTER	MAC PC
J013	2	LIBRARY/ C.LAB	COMPUTER	
J014	1	LIBRARY/ C.LAB	COMPUTER	MAC PC
J015		LIBRARY/ C.LAB		NOT USED
J016	2	LIBRARY/ C.LAB	PRINTER	
J017	1	LIBRARY/ C.LAB	PRINTER	
J018	2	10		NOT USED
J019	1	11	PHONE	CISCO IP
J020	2	11	COMPUTER	MAC PC
J021	2	11		NOT USED
J022				N/A
J023				N/A
J024	3	MPR	PHONE	CISCO IP
J025	1	MPR	COMPUTER	MC-PC
J026	1	MPR	COMPUTER	
J027	1	MPR		NOT USED
J028				N/A
J029	1	MPR	COMPUTER	
J030	1	MPR	COMPUTER	
J031	2	WORK RM	COMPUTER	
J032		WORK RM		NOT USED
J033				N/A
J034		WORK RM		NOT USED
J035		OFFICE		NOT USED
J036		HALLWAY		NOT USED
J037		HALLWAY		NOT USED
J038		HALLWAY		NOT USED
J039				
J040				
J041				
J042				
J043				
J044				
J045				
J046				
J047				
J048				

Appendix G
Advanced Data Communications
Network Discovery Audit Findings and Recommendations

BURLINGAME INTERMEDIATE SCHOOL

NETWORK DISCOVERY AUDIT

BURLINGAME SCHOOL DISTRICT (DO)

Findings:

- IDF/MDF is not in a secured closed room
- No labels on the patch panel, cables, faceplates, jacks
- Cable are Cat5 and Cat5e
- Cables coming from the location going to IDF is plugged in directly to switch

Recommendations:

- Provide a secure area for the IDF. It must be closed to control environment, security
- Old /abandoned cables must be removed from walls, IDF rack or closet and pathway for safety and not hazardous
- All patch panel must have labels including jack and cables for easy locating of data drops or station working on
- Cables coming from the work station should be punched into a patch panel
- Floor plan should be always in hand or should be mounted at the IDF to more quickly locate the station

BURLINGAME INTERMEDIATE SCHOOL (BIS)

Findings:

- IDF/MDF is not in a secured closed room
- Switches are only inside the closet not in the rack or enclosed box
- No labels on the patch panel, cables, faceplates, jacks
- Some cables are too long of a run
- Some cables are run straight to switch
- Cables are being pinched on the pathway by zip ties
- Some IDF are in attic space and closet

- Pathway or wire mold used at computer lab was too narrow so cables are being pinched
- MDF fiber panels are located in the wall

Recommendations:

- Provide a secure area for the IDF. It must be closed and secured in a controlled environment
- Old/abandoned cables must be removed from walls, IDF rack, closet and pathway for safety. This will limit fire hazard
- Uplink/backbone from IDF to MDF must be fiber for higher bandwidth
- Upgrade cables to Cat6 or higher for better performance
- Use Velcro to bundle cable
- MDF/IDF fiber panel should be mounted on the rack with the patch panels and switch
- Network components should be consolidated in same rack
- Wire mold and surface mount box should be screwed into the wall

FRANKLIN ELEMENTARY SCHOOL (FES)

Findings:

- IDF/MDF is not in a secured, closed room
- No labels on the patch panel, cables, faceplates, jacks
- Cables are Cat5 and Cat5e. Indoor cable was used for outside. Hence, some cables are deteriorating and getting loose connections
- Cables are more than the standard length (298 ft.)
- Cable coming from the location going to IDF is plugged in directly to switch
- IDF was warm and there is no vent to cool the area
- Materials used on pathways are not to code

Recommendations:

- Provide a secure area for the IDF. It must be closed to control environment, security
- Old /abandoned cables must be removed from walls, IDF rack or closet and pathway for safety and more space for new cables
- All patch panels must have labels including jack and cables to easily locate data drops or work on station
- Cables coming from the workstation should be punched into a patch panel
- Floor plan should be always in hand or mounted at the IDF to quickly locate the station

- Proper pathway materials should be used such as pipes and wire mold for indoor and wire management

LINCOLN ELEMENTARY SCHOOL (LES)

Findings:

- IDF/MDF is not in a secured closed room
- Switches are only inside the closet not in the rack or enclosed box
- Patch panels are in two different locations. Some are in the wall.
- No labels on the patch panel, cables, faceplates, jacks
- Some cables are too long of a run
- Some cables are run straight to switch
- Cables are being pinched on the pathway by zip ties

Recommendations:

- Provide a secure area for the IDF. It must be closed to control environment, security
- Old /abandoned cables must be removed from walls, IDF rack or closet and pathway for safety and more space for new cables
- All patch panels must have labels including jack and cables to easily locate data drops or work on station
- Uplink/backbone from IDF to MDF must be fiber for higher bandwidth
- Upgrade cables to Cat6 for better quality
- Use Velcro to bundle cables

McKINLEY ELEMENTARY SCHOOL (MES)

Findings:

- IDF/MDF is not in a secured, closed room
- Switches are only inside the closet, not in the rack or enclosed box
- Patch panels are in two different locations. Some are in the wall.
- No labels on the patch panels, cables, faceplates, jacks
- Network components such as patch panel, switch, fiber panel are not organized in standard positions
- IDFs are in a warm area like attic
- Cables are still in CAT5 and CAT5e

- Copper link from IDF to IDF

Recommendations:

- Provide a secure area for the IDF. It must be closed to control environment, security
- Old /abandoned cables must be removed from walls, IDF rack, closet and pathway for safety. This will limit fire hazard.
- Uplink/backbone from IDF to MDF must be fiber for higher bandwidth
- Upgrade cables to Cat6 or higher for better performance

ROOSEVELT ELEMENTARY SCHOOL (RES)

Findings:

- No labels on the patch panel, cables, faceplates, jacks
- Some cables are too long of a run
- No MAP on ID

Recommendations:

- Map or floor plan is needed at IDF side
- Cables should be standard length

WASHINGTON ELEMENTARY SCHOOL (WES)

Findings:

- IDF/MDF is not in a secured, closed room
- Patch panels are in two different locations; some are in the wall
- Network components such as patch panel, switch, fiber panel are not organized in standard positions
- Old cables are still in rack and behind some of the wall plates
- No labels on the patch panels, cables, face plates, jacks
- Some cables are CAT5, some are CAT5e

Recommendations:

- Provide a secure area for the IDF. It must be closed to control environment, security
- Old /abandoned cables must be removed from walls, IDF rack or closet and pathway for safety

- Rack must be assembled in an organized manner to have a better flow of cables and make it easier to find ports or jack
- All patch panels must have labels including jack and cables to easily locate data drops or work on station

Appendix H

Sample District
Disaster Recovery Plan

The following pages outline the recovery process for the ABC School District

****this document must be kept in paper form by the ****
****emergency recovery team****

1. Introduction

Planning for the business continuity of the ABC School District in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster **affecting the administration functions** of the school district requires the cooperative efforts of many support organizations in partnership with the functional areas supporting the "business" of ABC School District. This document records the Plan that outlines and coordinates these efforts.

For use in the event of a disaster, this document identifies the computer recovery facilities (hot sites) that have been designated as backups if the functional areas are disabled.

1.1 DEFINITION OF ADMINISTRATION FUNCTIONS

The following administrative functions are addressed by this plan:

- Payroll records and processing (description)
- Accounting records and processing (description)
- Student records and processing? (description)
- Equipment Inventory records and processing (description)
- District office processes (description)
- School building office processes? (description)
- Other

2. District Responsibilities

The following information outlines the responsibilities of the ABC School District.

2.1 OFF SITE STORAGE OF DATA AND SYSTEM MEDIA

What is stored; where it is stored; how often, by whom and how (physically moving tapes, backed-up over network, or other)

What? For example: payroll records, accounting records, invoicing records, equipment inventory records, board minutes, policy manuals, insurance policies, personnel records, county/auditor records, disaster recovery procedure, software application disks, hardware configuration disks, etc.…. Some are hard copies, others are soft. (What about school building office records? Student records, …)

Where? For example: at a remote school building; maybe reciprocal agreement with another district; regional agency

How often? Hard copies can be kept remotely and their existence verified quarterly through a simple written procedure. Soft copies which change often may be backed up once a week (or however often is determined locally) and moved to an off-site location as explained above, or just backed up over a network connection.

How long? LACA keeps copies of back-ups indefinitely (how far back can records truly be retrieved?) Legal requirements need to be researched.

By whom? Important to designate person/organization responsible

How? Tape media, hard copy, on-line accessible, microfiche, CD, etc…

2.2 ON SITE STORAGE OF DATA AND SYSTEM MEDIA

Define what is stored on site and how it is stored. i.e. Board minutes stored in fire-proof safe box, local district files stored on a local server, etc., paper documents stored in a filing cabinet, etc. Continue items from 2.1

2.3 DEFINITION OF SYSTEM(S)

Define the equipment, software, installation procedures and configurations, supplies and telecommunications necessary for all administrative operations.

Example: printing checks, direct deposit slips, purchase orders…
Wiring direct deposit
Client software/setup

2.4 DEFINE TEAMS AND RESPONSIBILITIES OF EACH

Define the following teams and responsibilities in the event of a disaster:

Data Team:

- Coordinates support for data processing resources at the main data center and designated recovery sites

Communications Team:

- Alternate voice and data communications capability
- News Media

- Human Resources elements of recovery and notify staff

Insurance Team:

- Physical plant – security, electrical, plumbing
- Liaison for insurance carriers

3. DIASASTER RECOVERY SERVICES

3.1 DISASTER RECOVERY SERVICES

As a member of the Licking Area Computer Association (LACA), the ABC School District automatically receives disaster recovery services from the organization.

LACA maintains two computer labs where access is available to all software applications/data contracted by the ABC School District.

It is the responsibility of ABC School District to outline all system definitions in section 2.3 and verify functionality with LACA and/or the school district "hot sites".

3.2 DISASTER RECIPROCAL AGREEMENT: ("HOT SITE")

The ABC school district has an agreement with all other member school districts of LACA (or pick one partnership district?) located in Licking and Muskingum Counties, Ohio.

This agreement stipulates that, in case of a disaster (where the computer equipment at our location is out of service), our users may have access to computers at the functioning locations so that our necessary *district business processes* may be performed.

NOTE

These arrangements are solely for the purpose of recovering business functionality in the event of a disaster, and are not intended for daily use by the non-functioning users.

LACA and the ABC School District Data Team will work cooperatively to make all the necessary arrangements in order to schedule those school districts users requesting services.

4. PRIORITY USAGE LIST OF "HOT SITE" USAGE

The following information outlines the priority in which users affected by the "disaster" may have access to the designated "hot site".

Define:

- Critical Functions: immediate need (ex: bi-weekly payroll)
- Essential Functions: what and how often (ex: accounting checks once a month)
- Necessary Functions: what and how often
- Desirable Functions: what and how often

**Sample plan:

1. Those users required to process payroll will be given priority over all other users.

2. Normal financial daily operations such as p/o, receipt, and check processing will be allowed access to the "hot site" on a bi-weekly basis. Student Services:

    a. Grade reporting will be given priority over all other student services operations;

    b. Attendance, and other reports will be allowed access to the "hot site" on a bi-weekly basis.

3. All other non-essential operations will cease until normal operations are restored.

5. RECOVERY PLAN

In the event of a disaster, the (specified district staff) will organize the disaster teams per Appendix A (and section 2.4) and implement the assignment of recovery tasks to the disaster team.

The following recovery plan will be implemented and followed until computer services normally provided by the district office are restored.

1. Define a central point of contact (disaster phone number will be established) and a record of all inbound/outbound calls will be made. (Communications Team)

2. Assess damage to hardware, software, and site. (Insurance Team)

3. Notify appropriate district staff with instructions, appropriate support agencies, i.e. LACA, LCESC, COSERC, ODE…. (Communications Team)

4. “Hot sites” will be notified of the situation and request made to implement this recovery plan. (Data Team)

5. All data media containing the necessary files, will be gathered from the off-site storage facilities (tapes, etc..) and steps followed per Appendix D: (Data Team)

    a. Latest “DAILY” backup (the most recent daily backup of the working week). Local servers

    b. Latest WEEKLY copy (and one week prior copy). Local servers

    c. Latest copy of all software.

6. Those users requesting services as outlined in Section 3 will notify the S.D. disaster phone number of their needs. S.D. will make arrangements with the “hot sites” to see that the requesting user has access available with them and to insure that the data files are then loaded (through LACA or local district) if not already available. (Data Team)

7. S.D. will maintain a staff member at a location convenient with the “hot site” to help the non-functioning district users. (Communications Team)

8. Necessary vendors and insurance companies are notified per Appendix B. (Insurance Team)

9. Backups are run at the “hot site” for those districts that have been utilizing the system. These are then stored as per outlined in Section 2.1. local servers (Data Team) 10. S.D. will publish a monthly schedule ensuring priority and equal biweekly shared access to the “hot site” and remote access locations. (Communications Team)

10. A new/repaired facility has been established and/or new equipment installed for school district operation. (Insurance Team)

11. All user files are brought up-to-date with the latest backup copies. Local servers (Data Team)

12. Users are notified of the location and hours of operation of the reinstalled, operational S.D. (Communications Team)

NOTE

Pending “hot site” and LACA approval, district personnel who wish to access the “hot site” through their own ISP connection may contact the S.D. Disaster phone number for assistance.

APPENDIX A

School Contact Personnel

Name	Position	Emergency Contact Number	Team
	Superintendent	Home: Cell:	
	Assistant Superintendent	Home: Cell:	
	Assistant Superintendent	Home: Cell:	
	Director of Technology	Home: Cell:	
	Etc…..		

APPENDIX B

CONTACT LIST - Vendors

Emergency Site – ABC School District

Banks

Software

Hardware (Servers, Computers/Workstations, Printers, Copiers, etc.)

Cisco Systems, Inc. (Network equipment)

Telecommunications (phones, cell phones, etc.)

Insurance Company

State Department of Education

Supplies (office, special forms, printer cartridges, etc.)

SERS

OBES

APPENDIX C

List of School Districts/Emergency Contacts

The Following pages list the Organizations/School Districts that partnership with/ support the ABC School District.

Agency	Contact Person	Contact Information

APPENDIX D

Steps for Recovering our Data

APPENDIX E

Detailed Equipment Inventory of District Buildings

APPENDIX F

Detailed Network Diagrams (network equipment/wiring)

APPENDIX G

Additional Backup and Recovery for On-Site Servers

Appendix I

FCMAT
FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
CSIS California School Information Services

FISCAL CRISIS & MANAGEMENT ASSISTANCE TEAM
STUDY AGREEMENT
December 9, 2011

The FISCAL CRISIS AND MANAGEMENT ASSISTANCE TEAM (FCMAT), hereinafter referred to as the Team, and the Burlingame School District, hereinafter referred to as the District, mutually agree as follows:

1. BASIS OF AGREEMENT

The Team provides a variety of services to school districts and county offices of education upon request. The District has requested that the Team provide for the assignment of professionals to study specific aspects of the Burlingame School District operations. These professionals may include staff of the Team, County Offices of Education, the California State Department of Education, school districts, or private contractors. All work shall be performed in accordance with the terms and conditions of this Agreement.

In keeping with the provisions of AB1200, the County Superintendent will be notified of this agreement between the District and FCMAT and will receive a copy of the final report. The final report will be published on the FCMAT website.

2. SCOPE OF THE WORK

A. Scope and Objectives of the Study

1. Review the district's organizational structure for technology support services and make recommendations for improvement.
2. Review the district's staffing for technology support services and make recommendations for improvement.
3. Review the district's delivery of administrative technology support services and make recommendations for improvement.
4. Review the district's delivery of instructional technology support services and make recommendations for improvement.
5. Conduct an end-to-end network discovery audit to fully document the district's network and identify network elements for replacement/upgrade.

6. Based on the output of the network discovery audit, provide recommendations regarding cabling that needs to be replaced or installed to improve network reliability and performance.
7. Based on the output of the network discovery audit, provide recommendations regarding network elements that need to be replaced, upgraded, and/or installed to improve network reliability and performance.
8. Based on the output of the network discovery audit, create a new WAN design that improves network reliability and performance. These documents shall include a map and descriptions of recommended backbone elements, maps and descriptions of recommended network elements for each site LAN, and recommended network element configurations.

B. Services and Products to be Provided

Orientation Meeting - The Team will conduct an orientation session at the District to brief District management and supervisory personnel on the procedures of the Team and on the purpose and schedule of the study.

On-site Review - The Team will conduct an on-site review at the District office and at school sites if necessary.

1. Exit Report - The Team will hold an exit meeting at the conclusion of the on-site review to inform the District of significant findings and recommendations to that point.

2. Exit Letter - The Team will issue an exit letter approximately 10 days after the exit meeting detailing significant findings and recommendations to date and memorializing the topics discussed in the exit meeting.

3. Draft Reports - Electronic copies of a preliminary draft report will be delivered to the District administration for review and comment.

4. Final Report - Electronic copies of the final study report will be delivered to the District administration following completion of the review.

5. Follow-Up Support – Six months after the completion of the study, FCMAT will return to the District, if requested, to confirm the District's progress in implementing the recommendations included in the report, at no cost. Status of the recommendations will be documented to the District in a FCMAT Management Letter.

3. PROJECT PERSONNEL

The study team will be supervised by Anthony L. Bridges, CFE, Deputy Executive Officer, Fiscal Crisis and Management Assistance Team, Kern County Superintendent of Schools Office. The study team may also include:

A.	Marisa Ploog, CPA	Fiscal Intervention Specialist
B.	Andy Prestage	Management Analyst
C.	To be determined	FCMAT Consultant

Other equally qualified consultants will be substituted in the event one of the above noted individuals is unable to participate in the study.

4. PROJECT COSTS

The cost for studies requested pursuant to E.C. 42127.8(d)(1) shall be:

A. $500.00 per day for each Team Member while on site, conducting fieldwork at other locations, preparing and presenting reports, or participating in meetings.

B. All out-of-pocket expenses, including travel, meals, lodging, etc. The District will be invoiced at actual costs, with 50% of the estimated cost due following the completion of the on-site review and the remaining amount due upon acceptance of the final report by the District.

Based on the elements noted in section 2 A, the total cost of the study is estimated at $18,000.

C. Any change to the scope will affect the estimate of total cost.

Payments for FCMAT services are payable to Kern County Superintendent of Schools - Administrative Agent.

5. RESPONSIBILITIES OF THE DISTRICT

A. The District will provide office and conference room space while on-site reviews are in progress.

B. The District will provide the following (if requested):

1. A map of the local area
2. Existing policies, regulations and prior reports addressing the study request
3. Current or proposed organizational charts

4. Current and two (2) prior years' audit reports
5. Any documents requested on a supplemental listing
6. Any documents requested on the supplemental listing should be provided to FCMAT in electronic format when possible.
7. Documents that are only available in hard copy should be scanned by the district and sent to FCMAT in an electronic format.
8. All documents should be provided in advance of field work and any delay in the receipt of the requested documentation may affect the start date of the project.

C. The District Administration will review a preliminary draft copy of the study. Any comments regarding the accuracy of the data presented in the report or the practicability of the recommendations will be reviewed with the Team prior to completion of the final report.

Pursuant to EC 45125.1(c), representatives of FCMAT will have limited contact with pupils. The District shall take appropriate steps to comply with EC 45125.1(c).

6. PROJECT SCHEDULE

The following schedule outlines the tentative dates for key study milestones:

Orientation:	December/January pending board approval
Staff Interviews:	to be determined
Exit Interviews:	to be determined
Preliminary Report Submitted:	to be determined
Final Report Submitted:	to be determined
Board Presentation:	to be determined
Follow-Up Support:	If requested

7. CONTACT PERSON

Name of contact person: Robert Clark, Assistant Superintendent

Telephone: (650) 259-3812 FAX: _____

E-Mail: rclark@bsd.k12.ca.us

Robert Clark 9 Dec 2011

Robert Clark, Assistant Superintendent — Date
Burlingame School District

December 9, 2011

Anthony L. Bridges, CFE — Date
Deputy Executive Officer
Fiscal Crisis and Management Assistance Team