FCMAT
FISCAL CRISIS & MANAGEMENT
ASSISTANCE TEAM

Central Unified School District

Technology Review

March 20, 2007

Joel D. Montero
Chief Executive Officer

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

March 20, 2007

Marilou Ryder, Superintendent
Central Unified School District
4605 N. Polk
Fresno, CA 93722

Dear Superintendent Ryder,

In August 2006, the Central Unified School District and the Fiscal Crisis and Management Assistance Team (FCMAT) entered into a study agreement for a review of the district's technology. Specifically, the agreement asked FCMAT to do the following:

1. Conduct a review of the district's technology support organizational structure and staffing allocations and make recommendations for improvement.
2. Assess the district's technology support services delivery mechanism and make recommendations for improvement.
3. Assess the district's distribution of network resources and make recommendations for improvement.

The attached final report contains the study team's findings and recommendations.

We appreciate the opportunity to serve you and we extend our thanks to all the staff of the Central Unified School District.

Sincerely,

Joel D. Montero
Chief Executive Officer

Table of Contents

Foreword iii

Introduction 1

Background *1*

Study Guidelines *1*

Study Team *2*

Executive Summary 3

Findings and Recommendations 5

Organization and Staffing *5*

Systems and Operations *15*

Educational Technology *21*

Planning and Standards *23*

Appendices 27

Foreword

FCMAT Background

The Fiscal Crisis and Management Assistance Team (FCMAT) was created by legislation in accordance with Assembly Bill 1200 in 1992 as a service to assist local educational agencies in complying with fiscal accountability standards.

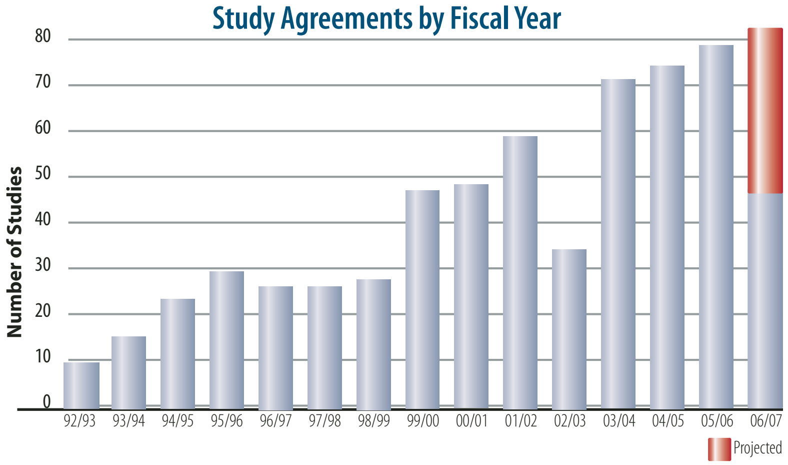
AB 1200 was established from a need to ensure that local educational agencies throughout California were adequately prepared to meet and sustain their financial obligations. AB 1200 is also a statewide plan for county offices of education and school districts to work together on a local level to improve fiscal procedures and accountability standards. The legislation expanded the role of the county office in monitoring school districts under certain fiscal constraints to ensure these districts could meet their financial commitments on a multiyear basis. AB 2756 provides specific responsibilities to FCMAT with regard to districts that have received emergency state loans. These include comprehensive assessments in five major operational areas and periodic reports that identify the district's progress on the improvement plans

Since 1992, FCMAT has been engaged to perform more than 600 reviews for local educational agencies, including school districts, county offices of education, charter schools and community colleges. Services range from fiscal crisis intervention to management review and assistance. FCMAT also provides professional development training. The Kern County Superintendent of Schools is the administrative agent for FCMAT. The agency is guided under the leadership of 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.

Total Number of Studies 628
Total Number of Districts in CA.......... 982

● Management Assistance............................	594	(94.59%)
● Fiscal Crisis/Emergency	34	(5.41%)

Note: Some districts had multiple studies.
● Districts (7) that have received emergency loans from the state.
(Rev. 2/7/07)



Introduction

Background

Located in the central San Joaquin Valley, the rapidly growing Central Unified School District covers approximately 88 square miles. Three departments reporting to two associate superintendents have evolved to support the district's software, hardware and communication networks. These departments develop and maintain a wide variety of customized software programs, reports and information systems. Various resources are hosted on 21 separate local area networks, 30 wireless networks, 40 servers and approximately 3,200 computer workstations. The district serves more than 1,200 employees and 14,000 students with this technology.

In August 2006, the Fiscal Crisis and Management Assistance Team (FCMAT) received a request from the district for a management review of its technology services. The scope and objectives of the technology review are to:

1. Conduct a review of the district's technology support organizational structure and staffing allocations and make recommendations for improvement.
2. Assess the district's technology support services delivery mechanism and make recommendations for improvement.
3. Assess the district's distribution of network resources and make recommendations for improvement.

Study Guidelines

A FCMAT study team visited the district on December 4, 2006 to conduct interviews, collect data and review documentation. This report is the result of those activities and is divided into the following sections.

I. Executive Summary

II. History

III. Organization and Staffing

IV. Systems and Operations

V. Educational Technology

VI. Planning and Standards

Study Team

The FCMAT study team was composed of the following members:

Andrew Prestage
Management Analyst
FCMAT
Bakersfield, CA

Robert Chambers*
Director, Technology Services
Rosedale Union School District
Bakersfield, CA

John Lotze
Public Information Specialist
FCMAT
Bakersfield, CA

Greg Lindner*
Director of Technology Services
Elk Grove Unified School District
Elk Grove, CA

Wade Williams*
Director, Technology & Learning Services
Stanislaus County Office of Education
Modesto, CA

* As members of this study team, these consultants were not representing their respective employers, but were working solely as independent consultants for FCMAT.

Executive Summary

District administrators have determined that stable and reliable technology resources are vital to continuing improvement in student performance. They also acknowledge the importance of timely and efficient technology support service delivery to maintain a robust instructional environment. An increasing backlog of support requests and frustration among instructional staff regarding unresolved technology issues has led to a review of technology support operations and staffing levels in the district. If implemented, the recommendations in this report will improve the efficiency and effectiveness of the district's technology support delivery.

The district's five year technology plan was developed without input from a wide range of district stakeholders, and schools do not have technology plans for their sites. The district's director of research, evaluation, assessment and technology (REAT) recently completed the update of the technology plan and is working to submit the plan prior to the April 2007 state deadline. The district should submit the five year plan for board approval and consider using a more thorough, collaborative and inclusive approach in future planning. Each school site should be required to develop a separate technology plan that supports the district's five year plan.

Technology services are currently fragmented, with three separate departments reporting to two assistant superintendents. As a result, communication, coordination standardization and combined planning and purchasing power are lacking. The district should consider combining the user services, student information systems, and research, evaluation, as-sessment and technology departments into a single department called Information Tech-nology Services (ITS), under the leadership of a new position titled Administrator of ITS reporting directly to the superintendent.

To ensure effective staffing for this new, combined department, the district should consider reclassifying some positions as follows:

- Consider reclassifying the research, evaluation, assessment and technology director position to administrator of ITS.
- Consider reclassifying the user services manager position to technical services di-rector, reporting to the administrator of ITS and overseeing user and technical ser-vices.
- Consider reclassifying one of the three micro computer specialist positions to server administrator, reporting to the director of technology services.
- Consider reclassifying the two remaining micro computer specialist positions to computer support specialists (CSS), reporting to the technology services manager.
- Consider reclassifying both of the current district technology aide positions as computer support specialists, bringing the total number of computer support specialist staff positions to four.
- Consider reclassifying the database manager position to student information systems manager, reporting to the administrator of ITS.

- Consider reclassifying and training the information systems database operator posi-tion to a help desk technician position, reporting to the SIS manager.

The district uses the Microsoft Access version of the Aeries student information system, which has caused performance issues. The district should migrate to the structured query language (SQL) version of the Aeries SIS to improve system performance.

Network and internet access and infrastructure is perceived as being unreliable and slow. The district should install additional T-1 lines for school sites and take other steps to increase the efficiency of the network.

Users do not have “home” directories or shared storage on the network for file sharing. These should be created.

FCMAT believes that support issues are underreported and that as the new combined department becomes more effective and communicates better, requests for support will increase. This potential trend should be monitored.

The district lacks technology support policies and procedures, as well as polices for equipment replacement, equipment donation and information technology security. As a result, there is a lack of consistency, costs may be higher than needed, and technology resources are distributed inequitably. Policies and procedures would help address these issues and should be developed.

Findings and Recommendations

Organization and Staffing

History

The Central Unified School District has enjoyed improved student achievement as a result of new strategic initiatives related to academics and district operations. The district's strategic initiative #4 is to "coordinate technology to improve student achievement" and is evidence of the administration's renewed interest in technology.

The district defined several strategies to help achieve this initiative, including the following:

- Update and implement the technology plan.
- Conduct a technology audit using the services of FCMAT.
- Align district resources with technology goals.
- Coordinate technology to enhance career and technical education.
- Provide teacher and employee staff development for greater technology efficacy.
- Provide technology equity across district, schools, grade levels and curricular areas.

FCMAT believes that the district's students will benefit from recent district efforts to update the five year technology plan using strategies that are realistic, attainable and measurable.

Technology Plan

The district's technology plan was recently updated by a limited number of staff, without input from a variety of district stakeholders. The district's director of research, evaluation, assessment and technology (REAT) recently completed the update of the district's technology plan and is working to submit the plan prior to the April 2007 state deadline.

The technology plan may not accurately reflect the district's vision and goals with respect to technology. For example, because technology support staff members were not involved in creating the plan, it does not address the priorities of technology service. In addition, none of the district sites have created site technology plans that support districtwide technology goals and initiatives.

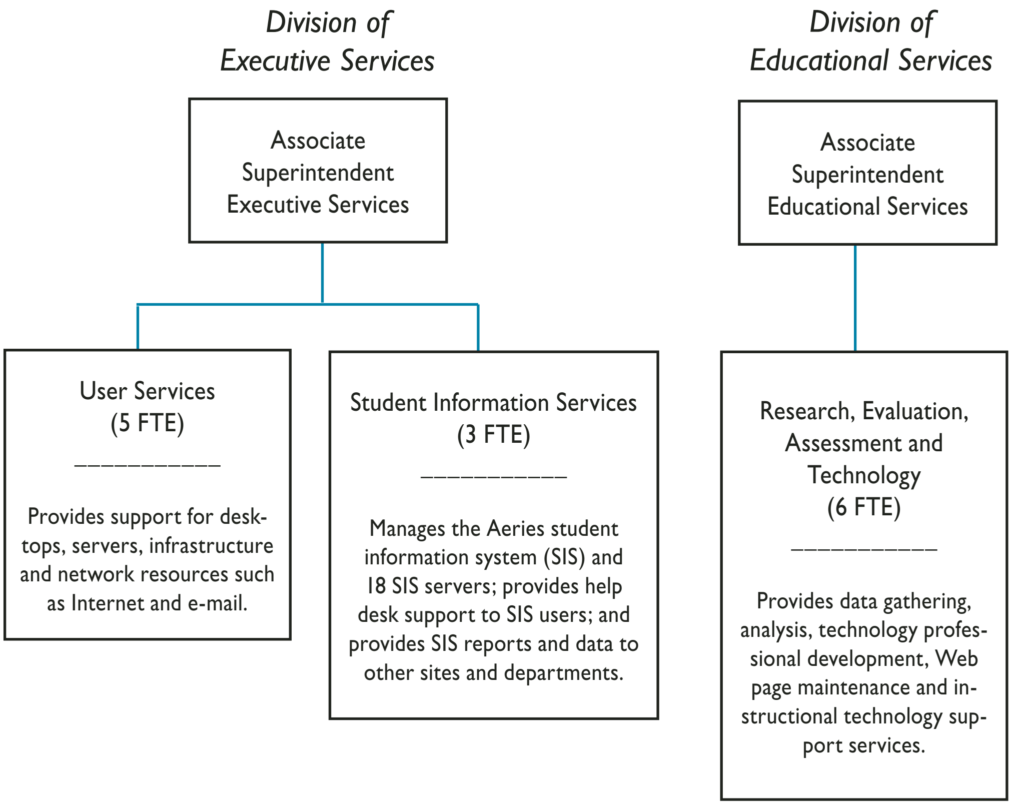
Although the development of the plan may have been expedient for grant and E-Rate funding requirements, the lack of broad participation in the creation of the new technology plan significantly limits its credibility and usefulness as a guiding document for the district.

Best practices for technology planning suggest that a technology planning team be established that includes representatives from many groups, including students, parents, teachers, library media specialists, resource specialists, site administrators, district administrators (curriculum and technology), classified staff, community leaders, business representatives and partners from higher education.

A broad-based technology committee should be formed to review and update the technology plan and other key technology issues. The committee should establish weekly meetings and should be chaired by a district instructional technology leader.

Three departments reporting to two associate superintendents have evolved to provide technology support services to district users. This fragmentation of technology support has created difficulties in the areas of technology leadership, responsibility, accountability, coordination, and communication. There is almost no communication between the three department leaders. The lack of coordination has created an environment in which site staff do not believe their concerns are taken seriously by technology department staff.

The following diagram shows the three departments' responsibilities and staffing levels, and indicates the administrative division to which each department reports.



Division of Executive Services

Associate Superintendent Executive Services

User Services (5 FTE)

Provides support for desktops, servers, infrastructure and network resources such as Internet and e-mail.

Student Information Services (3 FTE)

Manages the Aeries student information system (SIS) and 18 SIS servers; provides help desk support to SIS users; and provides SIS reports and data to other sites and departments.

Division of Educational Services

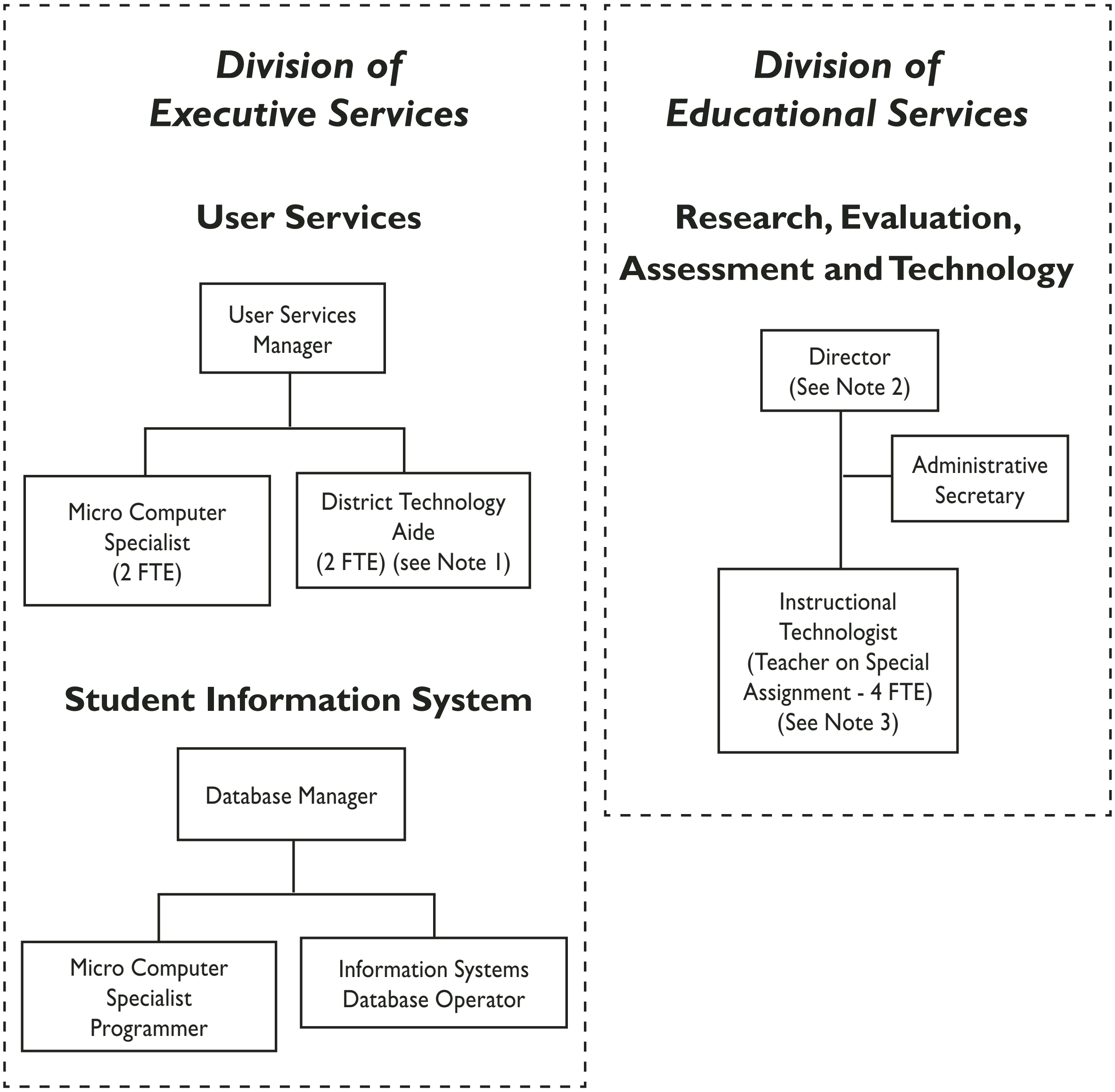
Associate Superintendent Educational Services

Research, Evaluation, Assessment and Technology (6 FTE)

Provides data gathering, analysis, technology professional development, Web page maintenance and instructional technology support services.

The two associate superintendents who oversee the district's technology services departments have different perspectives on technology services delivery and access to resources. For example, the executive services support division has a separate technology budget and support staff, and is primarily focused on system management, security, and user support. The educational services division has fewer technology support staff and is focused on data analysis and instructional technology. In addition, this division needs more access to network resources because of the needs of instructional technology users.

The following organizational charts depict staff positions within each of the three departments.


Division of Executive Services
User Services
User Services Manager
Micro Computer Specialist (2 FTE)
District Technology Aide (2 FTE) (see Note 1)
Student Information System
Database Manager
Micro Computer Specialist Programmer
Information Systems Database Operator
Division of Educational Services
Research, Evaluation, Assessment and Technology
Director (See Note 2)
Administrative Secretary
Instructional Technologist (Teacher on Special Assignment - 4 FTE) (See Note 3)

Note 1: One position currently vacant.
Note 2: Formerly a site administrator, recently assumed position following departure of prior director.
Note 3: One position currently vacant and frozen, pending outcome of FCMAT report.

User Services Department

The user services department primarily performs network and desktop support. One of the two micro computer specialist (MCS) positions is assigned to East High School and West High School, and the other is assigned to dispatch duties and district office support. The MCS job descriptions do not accurately describe the functions performed by these staff members, and the annual compensation of $42,000 associated with these positions may not be comparable to similar positions in neighboring school districts.

The two district technology aide positions, one of which is currently vacant, perform routine desktop support functions. The help desk software that the user services department uses to track and manage support requests is not used by either of the other two technology departments. User services staff members stated that there are between 40 and 50 outstanding support request tickets districtwide. This is an average of approximately 2.8 outstanding tickets for each of the district's 18 sites. Based on data gathered from school districts statewide, the average number of outstanding tickets per site is closer to seven. FCMAT believes that users are underreporting requests for support and that more timely and effective support services would result in a corresponding increase in requests for user support, particularly with the district's progress toward increased, and increasingly data-driven, instructional technology.

Despite the low number of reported support requests, the allocation of user support staff to school sites has resulted in an environment in which staff are constantly responding to urgent requests or emergencies. Because support staff have found it increasingly difficult to keep pace with the demand for support, most support is reactive rather than proactive. The district is unlikely to achieve an acceptable balance of control with the current support staff allocation arrangement.

Student Information Systems (SIS) Department

The student information systems (SIS) department provides Aeries student information system support, including data extracts and analysis as well as help desk and telephone support.

Cross-training of staff is lacking in both the user services department and the SIS department.

Research, Evaluation, Assessment & Technology Department

The research, evaluation, assessment and technology (REAT) department is comprised of a director and five full-time equivalent (FTE) positions. The administrative secretary position in this department is responsible for normal secretarial duties and some technology duties, including student system queries for school sites, packaging and scanning tests and following up on e-mails from users. A position of this type is not uncommon in a technology department. Some of the duties performed by the administrative secretary were formerly performed by another position, but the administrative secretary has been asked to perform these duties pending the outcome of this report.

Each of the REAT department's four FTE instructional technologist positions is filled by a teacher on special assignment (TOSA). One of the positions is currently vacant, and district administrators have opted not to fill the position pending the outcome of this report. Two of the instructional technologists are responsible for routine assessment duties typically performed by analysts in a research and evaluation department. The third position's duties are similar but include additional duties such as training and Web development and maintenance. The training is provided to the district's 15 site-based technology representative positions, which are filled by one certificated employee at each site who reports directly to the site administrator and receives an annual stipend of $600-800 to assist with technology support and training. During interviews, site staff indicated that the technology representatives are well regarded.

District administrators have recently begun to address the questions resulting from the fractured organizational structure of technology services, including the following:

- What level of technology service should the district's various technology support departments provide?
- Should all three departments be combined into a single large technology support department, or should the combined department size be kept small and each site given the responsibility for recruiting, employing, and training its own technology support staff?
- How should financial resources be allocated to address the inequities in technology infrastructure between older and newer sites?
- What organizational structure would provide the highest level of technology service possible in the most efficient and cost effective manner?
- To which position and through which division of the organization should the technology services department report? Should the department report through the division of executive services, educational services, a combination of both, or directly to the superintendent?

FCMAT believes that as the district's instructional technology becomes more widespread, its uses will become more diverse and more integral to student learning. When this occurs, the majority of the district's technology will be used for instructional purposes rather than administrative tasks, and the technology function will no longer fit neatly within either the executive or educational services division.

The central question to answer in defining a new reporting relationship is whether or not the three departments need to be consolidated into a single technology department. As currently configured, the administrative and instructional technology functions could continue to report within their respective divisions.

However, continued separation of the instructional and administrative technology functions into three departments reporting to separate divisions will make it more difficult to address essential technology issues, including establishing hardware and software standards, and providing support and training for all users.

Resolving these issues for both administrative and instructional technology will require a level of coordination that can best be provided if technology functions are overseen by a single department. FCMAT believes that this combined department best reports directly to the superintendent. Because the superintendent is the district's instructional leader, the superintendent's direct oversight of the department will enhance the development of instructional technology and its integration into the curriculum. Additional benefits of this structure include improved communication, collaboration, and distribution of technology resources. This structure would also convey the importance of decisions that affect administrative and instructional technology.

There is little or no communication between the user services department and the student information systems department. Although both departments report to the associate superintendent of executive services, meetings between the two departments are rare, usually taking place only if a serious breakdown has occurred. Combining the two departments would improve communication and coordination and reduce problems that arise when similar services are provided by different departments.

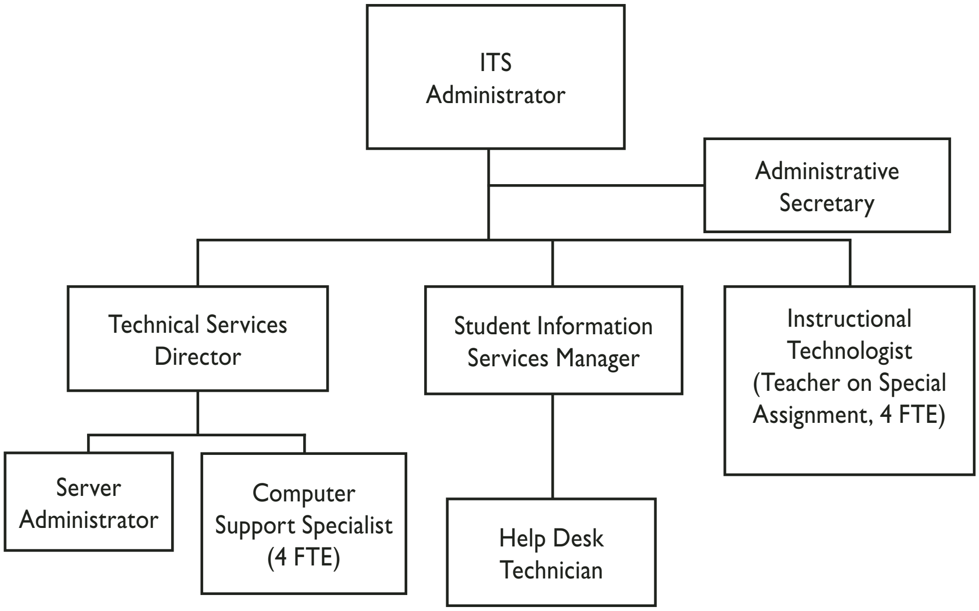
Recommendations

The district should:

1. Proceed with plans to submit the technology plan to the board of trustees to meet state deadlines for submission of the plan. Consider using a more thorough, collaborative, and inclusive approach to development of the technology plan in the future.
2. Immediately establish a technology planning team (TPT) consisting of key representatives from all district stakeholder groups. All managers responsible for providing technology support services should be members of the TPT.
3. Charge the TPT with reviewing and revising the newly developed five year technology plan. The TPT should adhere to technology planning guidelines set forth in the *Technology Planning Template* available from the TechSETS Web site at http://www.techsets.org/tools/tips.php?tip_id=4.
4. Require each school site to develop a separate technology plan that supports the district's plan. Site technology plans should be developed by site technology committees comprised of representatives from administrative, instructional and classified employee groups. The site plans should be developed after the district plan has been completed.
5. Ensure that all technology plans are approved by the board and updated annually to reflect current technology goals and objectives.
6. Consolidate the user services, student information systems, and research, evaluation assessment and technology departments into a single department called Information Technology Services (ITS).

The following sample proposed organization chart depicts all revised positions in the consolidated technology services department:

Information Technology Services


ITS Administrator
Administrative Secretary
Technical Services Director
Student Information Services Manager
Instructional Technologist (Teacher on Special Assignment, 4 FTE)
Server Administrator
Computer Support Specialist (4 FTE)
Help Desk Technician

7. Consider reclassifying the research, evaluation, assessment and technology director as Administrator of Information Technology Services. Consider having this position report directly to the superintendent. A sample ITS Administrator job description is included in Appendix D.
8. Consider reclassifying the user services manager position to Technical Services Director, reporting to the administrator of ITS. This position should be responsible for providing network engineering support including district communications; voice, video and data resources; Internet services; hardware and software standards; computer and printer support and repair; audiovisual support and repair; system integration; system administration; network configuration and documentation; systems training; system security; disaster recovery; and patch maintenance for all network devices such as routers, switches, firewalls and wireless access points. This position should supervise other technology support positions within the technology services department, as explained below. A sample technical services director job description is included in Appendix D.
9. Consider reclassifying one of the three micro computer specialist positions to server administrator, reporting to the director of technical services. This position should be assigned responsibility for server applications such as e-mail administration, the Aeries SIS, all server operating systems, server administration

and documentation, and network operating system support services for servers and users.

10. Consider reclassifying the two remaining micro computer specialist positions to computer support specialists (CSS), reporting to the technical services director. The technical services director should assign these positions to sites to provide hardware and software support, site modifications and installations, and desktop support, for all connectivity devices.

11. Consider reclassifying both of the current district technology aide positions as computer support specialists, bringing the total number of computer support specialist staff positions to four so that the TS department is able to handle the increase in support requests that is likely to arise from more timely and effective delivery of support services.

12. Consider allowing the currently unfilled district technology aide position, reclassified as a CSS position, to remain vacant for the short term to allow the new technical services director time to accurately determine support staffing requirements.

13. Develop a staffing allocation model based on site and infrastructure requirements to create a more balanced, controlled and proactive support delivery structure. Over time, this will reduce the number of unreported requests for support, increasing demands on technology support staff. The director of technical services should carefully monitor support demand during this period and retain the option of filling the remaining vacant CSS position if needed.

14. Consider reclassifying the database manager position to student information systems manager, reporting to the administrator of ITS. This position should continue to provide data analysis and extraction, and information support for users of the Aeries SIS.

15. Consider reclassifying and training the information systems database operator position to a help desk technician position, reporting to the SIS manager. Assign this position the responsibility of fielding SIS questions and providing first level desktop support to users. The intent of this position is to provide a single source of assistance to both instructional and administrative personnel. All calls should be logged in to the help desk software and all unresolved requests should be routed to more experienced technical support personnel at the sites or the district.

16. Ensure that cross-training is provided to user support and SIS support staff so that staff members are able to perform a variety of functions and ensure continuity of service.

17. The ITS administrator should continue to supervise the instructional technologist staff. The instructional technologist positions should be responsible for instructional support, desktop and network training, site services, video and

satellite services, technology training, library technology, software acquisitions, and site and district licenses.

18. Review the job description for the administrative secretary position to ensure that this staff member is not working out of class. Some of the duties performed by this position may be more commonly associated with those of an analyst in other research and evaluation departments. This position should continue to report to the ITS administrator.
19. Update the job description for the instructional technologist position to remove Web site development and maintenance tasks, and transfer these functions to the technical services department.
20. Continue to use the existing help desk application to manage support requests for the consolidated technology services department.
21. Consider conducting a comparative salary study of technology positions to determine if adjustments should be made.
22. Ensure that the technical services director and the student information systems manager meet regularly to discuss issues and improve communication.

Systems and Operations

The district uses the Microsoft Access database version of the Aeries student information system (SIS) rather than the structured query language (SQL) version. As a result, much of the work on the Aeries SIS uses Microsoft Access macros rather than built-in Aeries SQL queries. Use of the Access version is one of the major factors contributing to system performance complaints from SIS users.

Some users expressed frustration that it can take several minutes to retrieve student information from the SIS. Users characterized this as a bandwidth problem; however, it is more likely a result of known problems with the Aries software. The company commonly recommends running terminal services to resolve this issue.

The district lacks a technology support policy that defines service expectations and provides guidelines for the delivery of technology support services. An effective technology support policy would include the following service expectations:

- All telephone calls to the technology department will be answered by a staff member rather than by voicemail.
- Voicemail will be used only if desired by the caller and after the caller has been presented with other support alternatives.
- All e-mail support requests to the technology department will be responded to within 20 minutes of the time they are received.
- Every attempt shall be made to resolve support requests at the time of first contact from the user.
- Equipment loaned by the technology department shall be installed and operating within 24 hours of first contact from the user.
- Technology support staff members will inform users of when work is to be performed, what work is done, and updates on work progress or resolution.
- If a personal update cannot be provided to the user, the technology support staff member will leave a detailed note or provide a status update to the office staff prior to leaving a site. In addition, a follow-up e-mail message explaining the reason(s) for not providing support shall be sent to the appropriate site administrator, with copies to the assistant superintendent of business and assistant superintendent of education.
- Technology support staff members will check in with site office staff upon arrival and request information on items that require attention. They will also check out with site office staff prior to leaving, and provide an update on the status of work performed and information about what is being done to correct any remaining problem(s).
- Before the end of their shift, technology support staff members will send an e-mail message to the appropriate site administrator summarizing support activities performed and problems resolved for that day.

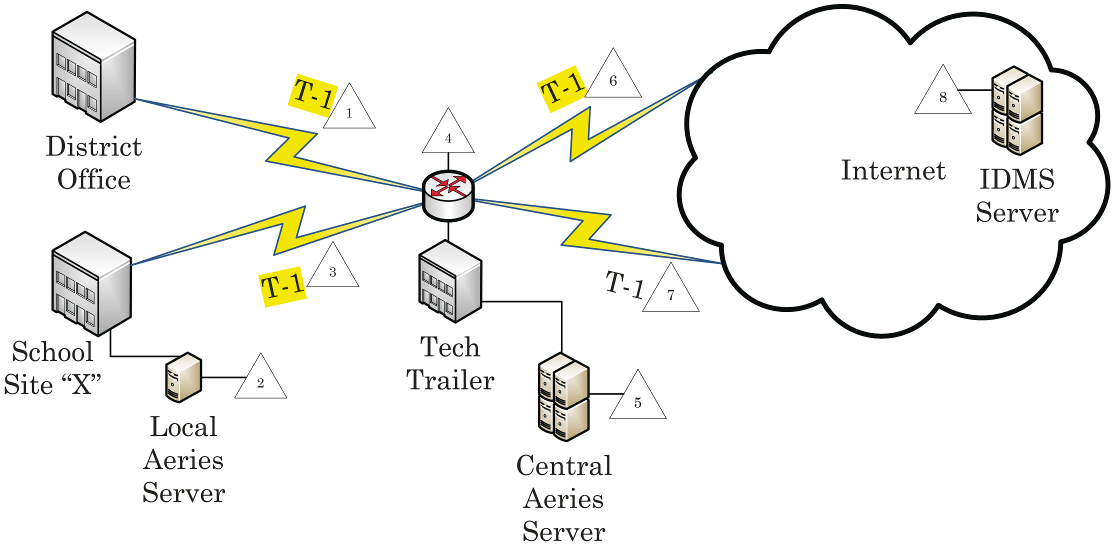
- Any planned support activity that requires shutting down a server or other communications equipment shall be preceded by a message at least one week in advance informing users of the time and duration of the planned outage.
- Planned network outages shall be preceded by three broadcast network messages, one four hours prior; one an hour prior and one five minutes prior to the outage.
- Any unplanned support activity that requires shutting down a server or other communications equipment shall be preceded by at least three broadcast network messages informing users of the time and duration of the emergency outage.

During interviews, staff members expressed frustration regarding a perceived lack of sharing of technology job knowledge and information. One staff member commented that the recent departure of two key staff members from the REAT department abruptly hampered the department's ability to provide information requested by site administrators. Best practices include sufficient cross-training of staff to ensure that the loss of any individual staff member does not significantly hamper operations.

Many staff members commented about the lack of system performance. The network infrastructure is perceived as being unreliable and slow. Technical staff indicated that the points of failure include faulty wiring, old routers and switches, and lack of bandwidth. Users commonly indicated that system performance problems were associated with a lack of available network bandwidth. The district's plans to relocate technology services staff members to the district office may provide an opportunity to conduct an in-depth review of the problems and determine the causes of the poor network performance. The table below summarizes the comments received by FCMAT regarding the performance of three critical district applications at three different locations.

	Technology Trailer	District Office	School Sites
IDMS	Fast	Fast	Slow
Aeries System	Fast	Slow	Fast
Internet	Fast	Fast	Slow

The diagram on the following page shows the basic configuration of the district's network and internet connectivity:



1 Users at the district office connect to the Technology Trailer via a dedicated T-1 line.
The overall transmission rate of a T-1 carrier connection is 1.544 million bits per second (Mbps).

2 Every school site has a local Aeries server that contains that site's student data.
Access to a local server significantly reduces the response required for data access.
Data is backed up to the central Aeries server (located at the Technology Trailer) on a nightly basis.

3 Users at each of the district's 18 school sites connect to the Technology Trailer via a dedicated T-1 line.

4 All Internet traffic district-wide flows through the district's core router located at the Technology Trailer.

5 The central Aeries server is the main repository of all student data for all 18 school sites.

6 Users at the district office connect to the Internet via a dedicated T-1 line.

7 Users from all 18 school sites connect to the Internet via a dedicated T-1 line.

8 The district's IDMS server is remotely hosted on the Internet. All access to this server is via a T-1 line.

From the information in the above diagram, the following conclusions can be drawn regarding system performance and bandwidth:

a. There are no problems associated with system performance or bandwidth from the technology trailer because access to the primary Aeries server is local, and access to the Internet and the Web-based instructional data management system (IDMS) is via a T-1 line that is used only by personnel at the district office and technology trailer.

b. Users at the district office have no problems with Internet connectivity and the IDMS because the district office has nearly exclusive access to a T-1 line. However, performance problems do exist for district office users of the Aeries student information system because of a known problem: Aeries software performance degrades significantly if data must be transferred across a wide area link such as exists between the district office and the technology trailer.

c. Users at school sites do not have problems with Aeries student data access because every site has a local Aeries server and data does not have to travel across any wide area links. However, there are system performance issues with Internet and IDMS use because all 18 school sites share a single T-1 line for Internet access. With as many as 4,000 workstations districtwide, the current single T-1 line is insufficient for Internet access and creates a significant communication bottleneck. Additional T-1 lines for school site traffic would significantly improve Internet and IDMS performance for site users, including instructional staff and students.

The district currently uses WebSense for Internet content filtering. It is possible that some filters may be incorrectly configured and may be slowing or blocking network traffic that does not need to be filtered.

It does not appear that the district uses shaping to improve the efficiency of network traffic that between school sites, the district office and the internet. Shaping is essential to ensure that communication lines are used efficiently. It would allow the district technology personnel to see exactly what network traffic is being transmitted over various lines and to allow, disallow, increase priority or decrease priority of applications. For example, the priority of IDMS traffic could be increased while the ability to download music could be blocked or limited.

Recommendations

The district should:

1. Migrate to the SQL version of the Aeries SIS to improve system performance. A detailed evaluation of the training and hardware requirements for successful migration should be completed in advance.
2. Develop and communicate a technology support policy that defines expectations for the delivery of support services.
3. Dedicate a minimum of three T-1 lines to Internet access once the move to the district office is complete. It is recommended that districts have one T-1 line for every 1,000 Internet-connected workstations.
4. Contact the Fresno County Office of Education for information on the cost of switching Internet service providers from AT&T to the county office. Because the county office is a node site for the K-12 High Speed Network (K-12HSN), it receives free internet services from the network and may be able to provide the district with increased throughput and reliability at a reduced cost. If Internet services are switched to the county office, the district should evaluate the cost of a 100MB or 1GB fiber optic connection to maximize bandwidth.
5. Evaluate internet filters to determine if they are improperly configured and thus slowing or stopping network traffic that does not require filtering. The district

can contact Daniel Scafuto, WebSense field engineer, at (619) 417-0825 for a free assessment and reconfiguration of the WebSense product if needed.

Programs that would help the district with load balancing the use of its T-1 line include the following:

- PacketShaper (www.packeteer.com)
- Total Traffic Control (http://www.lightspeedsystems.com)

7. Check routers at all sites to ensure that they have appropriate memory and processors for the amount of traffic they are handling. Upgrade or replace routers as required to accommodate existing traffic and anticipated increases in traffic over the next three years.

8. Ensure that all network switches are at least 10/100 MB capable; switches that are 10/100/1000MB are recommended.

9. Ensure that no hubs reside on the network. Because hubs share connections, they increase the number of data collisions and slow down the network.

9. Test all network wiring at each site and make repairs as needed until network performance reaches the appropriate level for the wire's certification type.

Educational Technology

Most students, instructional staff and site administrators do not have access to personal or "home" directories on file servers where they can store their work. In addition, there are no common directories that would permit document sharing. These network resources are easy to create and help increase communications among students, teachers and administrators.

Technology resources are not equitably distributed throughout the district. Some schools have new hardware and software in every classroom and others have very scarce resources, some of which are obsolete. This has resulted in a two-tiered environment with regard to computer and networking capabilities.

Without exception, instructional staff indicated a desire for increased professional development in the area of technology.

Recommendations

The district should:

1. Ensure that students, instructional staff and site administrators have access to "home" directories on file servers where they can share their work.
2. Provide consistent computer and network resources throughout the district by implementing technology standards for the following:
   - Computer, projector and printer hardware in the site office, classrooms, library, and computer labs.
   - Network connectivity to every classroom.
   - Instructional software for reading, math, and social studies that is suitable for the grade levels at the site.
3. Encourage instructional staff members to attend training sessions, in-service workshops and conferences that offer professional development opportunities in technology. Selected instructional technology leaders should attend annual conferences such as Computer Using Educators (CUE) at least every other year. In addition, the district's local California Technology Assistance Project (CTAP) representative can provide instructional staff with training and professional development resources.

Planning and Standards

For years, district sites have planned and purchased technology assets independently. As a result, disparate, incompatible systems have been implemented and the advantages of collective purchasing power have been lost. For example, 30 non-standard laptop computers were recently purchased by one school site, with an additional 70 units ordered since FCMAT's field work for this review. The school purchased the laptops even though they were told not to, but without the ability to enforce this decision the purchase order was allowed to go through. The presence of non-standard equipment on a network creates additional support costs. Technicians have to carry twice the number of software drivers, create twice as many images for a computer that has malfunctioned, and receive twice the amount of training to support the additional non-standard equipment.

Increased coordination of technology purchases would reduce expenditures, benefit schools and departments, and save site resources.

The lack of enforced standards has increased support problems for user services staff. Often, user services staff members are first made aware of a technology project only when they are contacted for support when installation problems occur.

Sites have been informed that technology support will not be provided for donated equipment. The refusal to provide this support can be defended because limited personnel and resources are available to support potentially incompatible hardware. However, this has created a perception among site administrators that the user services department makes decisions arbitrarily and without considering the merits of individual projects.

The district should adopt a cautious approach to accepting donated equipment. An equipment donation policy should be developed that allows the district to accept equipment that meets or exceeds minimum standards.

The district lacks an equipment replacement plan. Computers that are more than five years old are slow and cannot run the latest software or operating systems. A generally-accepted strategy is to replace a percentage of the district's equipment each year. For example, replacing the oldest 20% of all district equipment annually would result in all the district's computers being replaced every five years. This would help provide better standardization of equipment; allow for more accurate technology budgeting and planning; and reduce support costs, thus reducing the total cost of ownership.

The district needs to augment its existing technology policies with additional policies that include technology-related functions

The district's most recently built schools include proper networking infrastructure.

There has been no training for the district's technology support staff. Systems and support functions suffer when technology support staff do not seek professional development to keep current with technology developments. For example, the district's implementation of the Aeries Microsoft Access-based SIS has resulted in significant system performance issues. Training in the maintenance of the Aeries SIS might have allowed the district to make changes before system performance became an issue.

Network wiring is installed by licensed contractors with assistance from maintenance department staff members. This practice may be contributing to the district's network performance problems if the wiring has not been installed to industry standards.

California School Information Services (CSIS) processing requirements are taking up a considerable amount of personnel time in the student information systems department. District staff stated that approximately 70% of one FTE is spent performing tasks related to CSIS reporting and information processing. This may be the result of lack of training on the Aries system and should be investigated.

Recommendations

The district should:

1. Develop coordinated technology purchasing practices to ensure the maximum benefit from limited financial resources.
2. Review and enforce the standards used for hardware and software purchase approvals.
3. Develop an equipment donation policy that defines minimum specifications for donated computer equipment. Hardware that does not meet minimum standards should be rejected. A sample donation policy is included in Appendix A.
4. Develop a computer equipment disposal policy. A sample disposal policy is included in Appendix B.
5. Develop a variety of policies to address technology security, maintenance, and performance issues. These policies and procedures should cover the following:
    - Acceptable encryption
    - Anti-virus protection
    - System auditing
    - Automatically forwarded e-mail
    - Database credentials
    - Dial-in Access
    - Information Sensitivity
    - Internet DMZ equipment
    - Passwords
    - Remote access
    - Router security
    - Server security
    - Virtual private network (VPN)
    - Wireless communication

    A set of sample policies is included in Appendix C
6. Make the ITS administrator responsible for increasing communication with site administrators to ensure that they are aware of site technology initiatives

before equipment is donated, procured or delivered. Site administrators should understand that they cannot expect the technology services department staff to provide support for equipment obtained without their knowledge or input.

7. Develop an equipment replacement strategy that includes replacing the oldest 20% of all district equipment each year.
8. Establish a procedure for routine patch maintenance on servers to ensure that server upgrades are applied equitably across the district and that all servers remain current with the latest patch releases.
9. Borrow networking standards for new schools from other school districts that are growing. Revise the standards to meet the district's needs and provide them to the district's architects to ensure that the standards are included in new school site plans.
10. Immediately budget for training for all technology staff members on the major systems they are responsible for supporting. The new director of technology services should assess systems and necessary skills and create a detailed training plan. A good assessment tool is the Skills Matrix, which outlines the skills needed to support various school technology services. The matrix can be found on the TechSETS Web site at http://www.techsets.org/training/matrix.php.
11. Use only licensed low-voltage wiring contractors who are skilled in installing Category 5 and 6 wiring and fiber.
12. Work with CSIS representatives to determine if problems with processing CSIS information may be related to lack of training on the Aeries SIS.

Appendices

Appendix A: Sample Computer Equipment Donation Policy

Appendix B: Sample Computer Equipment Disposal Policy

Appendix C: Sample Information Technology Security Policies and Procedures

Appendix D: Sample Job Descriptions

Appendix E: Study Agreement

Appendix A
Sample Computer Equipment Donation Policy

Sample Computer Equipment Donation Policy

Central Unified School District (CUSD) appreciates offers to donate used computer equipment. The following guidelines apply to acceptance of donated equipment.

1. All equipment accepted by CUSD should be in good working order. If the equipment is not in good working order, the accepting department or school assumes responsibility for the costs of putting the equipment in good working order.

   Comment: Often a donor wishes to dispose of equipment that is not in working order. They may have the belief that giving it to CUSD is a positive way to dispose of it and that the district can make use of it. Unfortunately, there are often significant costs the district would incur to return the equipment to working order. For this reason, it is generally advisable to decline equipment that is not in initial good working order. Technology department staff members may be able to assist district personnel in determining whether a potential donation is in good working order.

2. Whenever possible, accept only equipment that is supported by CUSD, as defined in the hardware and networking sections of the district Technology Plan document. If the equipment is fully supported by CUSD and is in good working order when received, then the district will maintain the equipment just as if it had been originally purchased by the district. If the equipment is not a supported item, the school or department that accepts the donation assumes responsibility for costs of keeping the equipment in good working order.

   Comment: Costs for repairing a piece of equipment that the district does not service can be substantial. Replacement of a computer motherboard or hard disk drive, for example, could cost more than the actual value of the equipment itself. In some cases, donated equipment can be viewed as “disposable,” with the intent to use it until it ceases to function, and then dispose of it.

3. Technology department staff members can assist with the setup and configuration of donated equipment that complies with the district hardware standards.
   For equipment that does not comply with the standards, technology support technicians can assist with the setup and configuration as long as the time required does not substantially exceed what would be required to set up equipment that is in compliance with district standards. If the technicians determine that extraordinary time will be required to set up and configure a non-standard piece of hardware, they will advise the accepting department or school that assistance will not be available.

Comment: Non-standard equipment can present serious challenges when interconnecting with district systems and networks. A substantial amount of time can be spent trying to locate software drivers and troubleshoot systems to make them work properly with other district systems. At some point the time invested to set up and configure the equipment exceeds the value of the equipment.

3. Donated network equipment should not be connected to the district network without specific permission and direction from district network support technicians. Donated computers should only be connected to a network after review and approval by district technicians.

   Comment: Networks are complex systems that require careful design and maintenance. The district strives to install networks that will be reliable and stable. A piece of networking equipment that is malfunctioning or improperly installed can destroy the integrity of the entire network and cause a network failure that impacts many students, staff and services. Under no conditions should anyone connect a hub, switch, router, or other device that affects the topography of a network without direct permission and direction from district network support technicians. Donated computers may contain network cards that are incompatible with district systems. Always check with an IT technician before attempting to connect an untested device to the network. Failure to do this may cause failure of your site network or even the entire wide area network. Technology department technicians are instructed to remove and/or confiscate unauthorized devices connected to any district network.

4. Make sure the donor provides software licenses for any donated software, including the operating system software.

   Comment: The district makes every effort to be in compliance with copyright laws. If software is loaded on a computer, proof of ownership or license for that software must also be provided. It is not uncommon for a donor to donate a computer that has the Windows operating system and copies of other commercial software already installed. Without proof of license, these software items must be removed or purchased by the district. Since every computer requires an operating system, be sure to understand if you are getting a license for Windows with the computer (Macintosh computers always retain their original OS license), or if the donor has retained the license. If the donor has retained the license for Windows (or never had a legal license), a copy will need to be purchased before the computer can be used. This cost should be considered before accepting the donation.

5. If the donor requires a receipt for their donation, provide them with a letter listing the make, model and serial number of donated items. It is the responsibility of the donor, not CUSD, to determine the value of donated items.

   Comment: A simple thank-you letter that lists the items that have been donated are appreciated by most donors and useful in many cases for tax purposes. It is not the responsibility of CUSD personnel to provide the donor with the appraised value of the equipment.

7. Items offered for donation at the district level will be reviewed by technology department staff for acceptance. Distribution of donated items to departments or schools will be handled by Assistant Superintendent. A donor may choose to designate a specific school or department to receive the donated items. If undesignated, the Assistant Superintendent will determine appropriate distribution by an assessment of need, or by soliciting proposals for usage of the equipment and selecting the recipient(s) on the merit of their proposal(s). A school or department may accept a donation directly if guidelines in this document are followed.

8. Any donated computer equipment, regardless of value, or other items valued at over $500 should be added to the fixed assets system. Final recipient of donated equipment should provide a list, including the source of the donation, serial numbers, descriptions, models, brands, and approximate values to appropriate personnel in the Business Office whereupon bar codes will be provided for the recipient to attach to the equipment for inventory control purposes.

9. Technology department staff members can answer questions about the advisability of accepting donations.

Appendix B: Sample Computer Equipment Disposal Policy

Sample Computer Equipment Disposal Policy

All surplus district-owned computers, faxes, copy machines, cell phones, and other electronic equipment with printed circuit boards shall be recycled by the district's selected and approved vendor. In addition, all computers or servers declared surplus that contain hard drives shall be wiped clean to at least DOD Level 3 or shall be destroyed by magnetic degaussing.

Rationale:

The State of California recently determined that discarded televisions and computer monitors are classified as hazardous waste, unless properly recycled by a state licensed facility. Monitors and terminals contain from 4 to 8 pounds of lead, and circuit boards of both computers and printers contain lead solder, mercury and cadmium. The proper disposal of this equipment is essential to avoid liability and to be an environmentally responsible corporate citizen. In addition, computer hard disks may contain personal, confidential, and legally protected information that is still readable even when the files have been erased or the hard drive reformatted. Failure to destroy this information could lead to unauthorized access, identity theft, and liability to the district.

The key points of this policy include:

1. All non-working /obsolete computer products should be disposed of in an environmentally sound manner

2. Monitors and terminals are always a hazardous waste (or household hazardous waste, if from household use).

3. Other components of a computer system (e.g., circuit boards, keyboards, mice) could be hazardous depending on their lead, mercury, or cadmium content, which can vary from product to product.

Procedure:

- Sites or departments that wish to declare computer equipment surplus shall send an e-mail to the Technology Department listing description, serial number, asset tag number, and operational condition of the unit(s).
- Equipment will be picked up by Technology Department staff.
- Technology Department staff will package and ship the equipment to a center where it will be recycled in an environmentally safe and responsible manner.
- The hard drive will be overwritten to at least DOD Level 3 standards, or will be destroyed by magnetic degaussing upon request.

Appendix C: Sample Information Technology Security Policies and Procedures

.

Sample

Orange County Department of Education
Information Technology Division
Information Security Policy and Procedures

The Orange County Department of Education's Information Technology Division understands the importance of information security and has adopted these Policy and Procedures as a measure to ensure the integrity and confidentiality of the data and information that is collected, processed and presented.

In addition to the mission and values of the Orange County Department of Education, the Information Technology Division has a commitment to protect all data collected against misuse of FRAUD and IDENTITY THEFT.

These Policy and Procedures were adapted from the SANS Institute – Security Policy Project and were modified to meet the needs of the Orange County Department of Education. The Policy and Procedures will continue to evolve and change as necessary to accommodate the changing technology.

Table of Contents

Acceptable Encryption Policy and Procedures ……………………
Anti-Virus Policy and Procedures ……………………………….
Audit Policy and Procedures ……………………………………..
Automatically Forwarded E-mail Policy and Procedures ………….
DataBase Credentials Policy and Procedures……………………...
Dial-In Access Policy and Procedures …………………………….
Information Sensitivity Policy and Procedures ……………………
Internet DMZ Equipment Policy and Procedures …………………
Password Policy and Procedures ………………………………….
Remote Access Policy and Procedures ……………………………
Router Security Policy and Procedures ……………………………
Server Security Policy and Procedures ……………………………
Virtual Private Network (VPN) Policy and Procedures ………….
Wireless Communication Policy and Procedures …………………

Orange County Department of Education
Information Technology Division
Information Security Policy and Procedures

Security/Confidentiality Agreement

Due to the nature and confidentiality of information, all staff in the Information Technology Division is required to read, understand, sign and date the Security Agreement. A copy of the Security Agreement will be kept in the employee's personnel file during employment with the Orange County Department of Education's Information Technology Division.

The term of the agreement is for one year and is subject to review annually. A sample of the agreement is in Appendix A.

Orange County Department of Education
Information Technology Division
Acceptable Encryption Policy and Procedures

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies to transfer files between the Orange County Department of Education Information Technology Division and other agencies.

2.0 Scope

This policy applies to all Orange County Department of Education Information Technology Division employees.

3.0 Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. Orange County Department of Education's Information Technology Division key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Orange County Department of Education Information Technology Division. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

All servers that are located within the Orange County Department of Education's Data Center that contain any information are required to maintain an encryption algorithm. The minimum requirement is SSL. Verisign digital certificates are also acceptable.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any agency found to have violated this policy may be subject to a hearing to determine appropriate actions.

5.0 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Orange County Department of Education
Information Technology Division
Policy and Procedures on Anti-Virus

1.0 Purpose

The purpose of this policy is to provide guidance in the use and selection of Anti-Virus software that protects the transmission of information via e-mail relatively free from viruses transmitted by electronic means.

2.0 Scope

This policy applies to all Orange County Department of Education Information Technology Division employees.

3.0 Policy

Anti-Virus software shall be installed, updated and maintained on all workstations that are connected to the Orange County Department of Education's network. Records and logs should be reviewed monthly for current status of software and are subject to review by senior management. In addition, anti-virus software shall be reviewed every two years to determine its features and its implementation at the Orange County Department of Education.

4.0 Recommended processes to prevent virus problems:

- NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk e-mail without forwarding, in accordance with Orange County Department of Education's *E-mail Policy.*
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., e-mail or file sharing.
- New viruses are discovered almost every day.

5.0 Revision History

Orange County Department of Education
Information Technology Division
Audit Vulnerability Scan Policy and Procedures

1.0 Purpose

The purpose of this agreement is to set forth our agreement regarding network security scanning offered by the Information Technology Division of the Orange County Department of Education. The Information Technology Division shall utilize approved and appropriate software to perform electronic scans of Client's networks and/or firewalls or on any system at the Orange County Department of Education.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to the Orange County Department of Education security policies
- Monitor user or system activity where appropriate.

2.0 Scope

This policy covers all computer and communication devices owned or operated by Orange County Department of Education. This policy also covers any computer and communications device that are present on Orange County Department of Education premises, but which may not be owned or operated by Orange County Department of Education. The Information Technology Division will not perform Denial of Service activities.

3.0 Policy

When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of the Information Technology Division. Orange County Department of Education hereby provides its consent to allow the Information Technology Division to access its networks and/or firewalls to the extent necessary to allow the Information Technology Division to perform the scans authorized in this agreement. Orange County Department of Education shall provide protocols, addressing information, and network connections sufficient for the Information Technology Division to utilize the software to perform network scanning.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Orange County Department of Education equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Orange County Department of Education networks.

3.1 Network Control. Not Applicable

3.2 Service Degradation and/or Interruption.
Network performance and/or availability may be affected by the network scanning.

3.3 Client Point of Contact During the Scanning Period. Not Applicable

3.4 Scanning period
Orange County Department of Education and the Information Technology Division Scanning Team shall identify in writing the allowable dates for the scan to take place.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Orange County Department of Education
Information Technology Division
Automatically Forwarded E-mail Policy and Procedures

1.0 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope

This policy covers automatic e-mail forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Orange County Department of Education.

3.0 Policy

Employees must exercise utmost caution when sending any e-mail from inside Orange County Department of Education to an outside network. Sensitive information, as defined in the *Information Sensitivity Policy*, should not be forwarded via any means, unless that e-mail is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*. All e-mail shall also conform to the established E-mail Policy within the Orange County's Department of Education's Policies and Procedures Manual.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
E-mail	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora, Microsoft Outlook or Lotus Notes use SMTP.
Forwarded e-mail	E-mail resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to Orange County Department of Education or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

6.0 Revision History

Orange County Department of Education
Information Technology Division
Database Password Policy and Procedures

1.0 Purpose

This policy states the requirements for securely storing and retrieving database user names and passwords (i.e., database credentials) for use by a program that will access a database running on one of the Orange County Department of Education's networks.

Computer programs running on Orange County Department of Education's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2.0 Scope

This policy applies to all software that will access an Orange County Department of Education, multi-user production database.

3.0 Policy

3.1 General

In order to maintain the security of Orange County Department of Education's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2 Specific Requirements

3.2.1. Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy.*

3.2.2. Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs should not be allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy.*
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy.* This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4. Coding Techniques for implementing this Policy

Passwords in any form should not be contained in software code that is developed by the Orange County Department of Education's Information Technology Division.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.

Executing body The series of computer instructions that the computer executes to run a
program.

Hash An algorithmically generated number that identifies a datum or its
location.

LDAP Lightweight Directory Access Protocol, a set of protocols for accessing information directories.

Module A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.

Name space A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.

Production Software that is being used for a purpose other than when software is being implemented or tested.

6.0 Revision History

Orange County Department of Education
Information Technology Division
Dial-In Access Policy and Procedures

1.0 Purpose

The purpose of this policy is to protect Orange County Department of Education's electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

2.0 Scope

The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

3.0 Policy

Orange County Department of Education Information Technology Division employees and authorized third parties (customers, support staff etc.) will be allowed to use dial-in connections to gain access to the corporate network under specific circumstances. Any Dial-in access is strictly controlled, using one-time password authentication. Dial-in access is only granted under the completed Dial-in access request form. Currently, Dial-in access is restricted to Information Technology support staff only.

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to Orange County Department of Education is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and Orange County Department of Education are literal extensions of Orange County Department of Education's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect Orange County Department of Education's assets.

Analog and non-GSM digital cellular phones cannot be used to connect to Orange County Department of Education's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to Orange County Department of Education's network. For additional information on wireless access to the Orange County Department of Education network, consult the *Wireless Communications Policy.*

Note: Dial-in accounts are considered **'as needed'** accounts. Account activity is monitored, and if a dial-in account is not used for a period of time the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Orange County Department of Education
Information Technology Division
Ethics Policy

1. **Overview**

   Orange County Department of Education Information Technology Division purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Orange County Department of Education employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

   Orange County Department of Education Information Technology Division is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Orange County Department of Education Information Technology Division addresses issues proactively and uses correct judgment, it will help set us apart from the rest.

   Orange County Department of Education Information Technology Division will not tolerate any wrongdoing or impropriety at anytime. Orange County Department of Education Information Technology Division will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. **Purpose**

   Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3. **Scope**

   This policy applies to employees at the Orange County Department of Education Information Technology Division.

4. **Policy**

   4.1. **Executive Commitment to Ethics**

   4.1.1. Senior executives within the Orange County Department of Education's Information Technology Division must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

   4.1.2. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

   4.1.3. Executives must disclose any conflict of interests regard their position within Orange County Department of Education Information Technology Division.

   4.2. **Employee Commitment to Ethics**

4.2.1. Orange County Department of Education Information Technology Division employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

4.2.2. Every employee needs to apply effort and intelligence in maintaining ethics value.

4.2.3. Employees must disclose any conflict of interests regard their position within the Orange County Department of Education Information Technology Division.

4.2.4. Employees will help the Orange County Department of Education Information Technology Division to increase customer satisfaction by providing quality products/services and timely response to inquiries.

4.3. **Company Awareness**

4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2. Orange County Department of Education's Information Technology Division will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the Division.

4.4. **Maintaining Ethical Practices**

4.4.1. Orange County Department of Education Information Technology Division will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2. Employees at Orange County Department of Education Information Technology Division should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.5. **Unethical Behavior**

4.5.1. Orange County Department of Education Information Technology Division will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2. Orange County Department of Education Information Technology Division will not tolerate harassment or discrimination.

4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our organization will not be tolerated.

4.5.4. Orange County Department of Education Information Technology Division will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.5.5. Orange County Department of Education Information Technology employees will not use corporate assets or business relationships for personal use or gain.

5. Enforcement

5.1. Any infractions of this code of ethics will not be tolerated and the Orange

County Department of Education Information Technology Division will act quickly in correcting the issue if the ethical code is broken.

5.2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

Orange County Department of Education
Information Technology Division
Information Sensitivity Policy and Procedures

1.0 Purpose

The Information Sensitivity policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the Orange County Department of Education Information Technology Division without proper authorization.

The information covered in these policy and procedures includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling policy and procedures that follow this introduction. It should be noted that the sensitivity level definitions were created as policy and procedures and to emphasize common sense steps that you can take to protect the Orange County Department of Education Confidential information (e.g., Orange County Department of Education Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these policy and procedures on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these policy and procedures should be addressed to the Information Technology Division Managers and/or Directors.

2.0 Scope

All Orange County Department of Education information is categorized into two main classifications:

- Orange County Department of Education Public
- Orange County Department of Education Confidential

Orange County Department of Education Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Orange County Department of Education.

Orange County Department of Education Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as personal information, payroll information and/or financial information. Also included in Orange County Department of Education Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Orange County Department of Education Confidential information is "Orange County Department of Education Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to the Orange County Department of Education by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Orange County Department of Education's network to support our operations.

Orange County Department of Education personnel are encouraged to use common sense judgment in securing Orange County Department of Education Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy and Procedures

The Sensitivity Policy and Procedures below provides details on how to protect information at varying sensitivity levels. Use these Policy and Procedures as a reference only, as Orange County Department of Education Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Orange County Department of Education Confidential information in question.

3.1 Minimal Sensitivity: General corporate information; some personnel and technical information

Marking Policy and Procedures for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Orange County Department of Education Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Orange County Department of Education Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Orange County Department of Education information is presumed to be "Orange County Department of Education Confidential" unless expressly determined to be Orange County Department of Education Public information by a Orange County Department of Education employee with authority to do so.

Access: Orange County Department of Education employees, contractors, people with a business need to know.
Distribution within Orange County Department of Education: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Orange County Department of Education internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase white boards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Orange County Department of Education premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 More Sensitive: Business, financial, technical, and most personnel information

Marking Policy and Procedures for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Orange County Department of Education Confidential" or "Orange County Department of Education Proprietary", wish to label the information "Orange County Department of Education Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Orange County Department of Education employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within Orange County Department of Education: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Orange County Department of Education internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within Orange County Department of Education, but should be encrypted or sent via a private link to approved recipients outside of Orange County Department of Education premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on Orange County Department of Education premises; electronic data should be expunged/cleared. Reliably

erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking Policy and Procedures for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Orange County Department of Education Confidential information is very sensitive, you may should label the information "Orange County Department of Education Internal: Registered and Restricted", "Orange County Department of Education Eyes Only", "Orange County Department of Education Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Orange County Department of Education Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Orange County Department of Education employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within Orange County Department of Education: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of Orange County Department of Education internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within the Orange County Department of Education but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Orange County Department of Education premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to Orange County Department of Education from an outside business connection. Orange County Department of Education computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Orange County Department of Education corporate information, the amount of information at risk is minimized. Unauthorized personnel accessing the Internet must use designated workstations in public areas such as the break rooms that are connected on the public side of network.

Configuration of Orange County Department of Education to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the Information Technology Division.

Approved Encrypted e-mail and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Orange County Department of Education is done via a license. Please contact the Information Technology Division if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of the Orange County Department of Education.

Encryption

Secure Orange County Department of Education sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate Policy and Procedures on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that Orange County Department of Education has control over its entire distance. For example, all Orange County Department of Education networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. Orange County Department of Education also has established private links to other agencies, so that all correspondence can be sent in a more secure manner.

Revision History

Orange County Department of Education
Information Technology Division
Internet DMZ Equipment Policy and Procedures

1.0 Purpose

The purpose of this policy is to define standards to be met by all equipment owned and/or operated by Orange County Department of Education Information Technology Division located outside the Orange County Department of Education's corporate Internet firewalls. These standards are designed to minimize the potential exposure to Orange County Department of Education from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of Orange County Department of Education resources.

Devices that are Internet facing and outside the Orange County Department of Education firewall are considered part of the "demilitarized zone" (DMZ) and are subject to this Policy. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

2.0 Scope

All equipment or devices deployed in a DMZ owned and/or operated by Orange County Department of Education Information Technology Division (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by the Orange County Department of Education Information Technology Division, must follow this policy.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from the Orange County Department of Education Information Technology Division.

3.0 Policy

3.1. Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by the Orange County Department of Education Information Technology Division for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the corporate wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of the Orange County Department of Education upon demand, per the *Audit Policy.*
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify compliance with this policy, Orange County Department of Education Information Technology Division will periodically audit DMZ equipment per the *Audit Policy.*

3.2. General Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by the Orange County Department of Education Information Technology Division as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards
- All patches/hot-fixes recommended by the equipment vendor and the Orange County Department of Education Information Technology Division must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by the Orange County Department of Education Information Technology Division.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by The Orange County Department of Education Information Technology Division) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords (DES/SofToken) must be used for all access levels.
- All host content updates must occur over secure channels.

- Security-related events must be logged and audit trails saved to the Orange County Department of Education Information Technology Division-approved logs. Security-related events include (but are not limited to) the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.
- The Orange County Department of Education Information Technology Division will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.3. New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the *DMZ Equipment Deployment Process*.
- Configuration changes must follow the Orange County Department of Education Information Technology Division's Change Management (CM) Procedures.
- The Orange County Department of Education's Information Technology Division must be invited to perform system/application audits prior to the deployment of new services.
- The Orange County Department of Education's Information Technology Division must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

3.4. Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	**Definitions**
DMZ (de-militarized zone)	Any untrusted network connected to, but separated from, the Orange County Department of Education's corporate network by a firewall, used for external (Internet/partner, etc.) access from within the Orange County Department of Education, or

to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.

Secure Channel — Out-of-band console management or channels using strong encryption according to the *Acceptable Encryption Policy.*. Non-encrypted channels must use strong user authentication (one-time passwords).

Untrusted Network — Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

6.0 Revision History

Orange County Department of Education
Information Technology Division
Password Policy and Procedures

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Orange County Department of Education's entire corporate network. As such, all Orange County Department of Education Information Technology Division's employees (including contractors and vendors with access to Orange County Department of Education systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Orange County Department of Education facility, has access to the Orange County Department of Education network, or stores any non-public Orange County Department of Education information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Information Technology Division's administered global password management database.
- All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the Policy and Procedures described below.

4.2 Policy and Procedures

A. General Password Construction Policy and Procedures

Passwords are used for various purposes at Orange County Department of Education. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words “Orange County Department of Education”, “sanjose”, “sanfran” or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for Orange County Department of Education accounts as for other non-Orange County Department of Education access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don’t use the same password for various Orange County Department of Education access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Orange County Department of Education passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Orange County Department of Education information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an e-mail message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.

- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the Orange County Department of Education Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Orange County Department of Education
Information Technology Division
Remote Access Policy and Procedures

1.0 Purpose

The purpose of this policy is to define standards for connecting to Orange County Department of Education's network from any host. These standards are designed to minimize the potential exposure to Orange County Department of Education from damages which may result from unauthorized use of Orange County Department of Education resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Orange County Department of Education internal systems, etc.

2.0 Scope

This policy applies to all Orange County Department of Education Information Technology Division employees, contractors, vendors and agents with a Orange County Department of Education -owned or personally-owned computer or workstation used to connect to the Orange County Department of Education network. This policy applies to remote access connections used to do work on behalf of Orange County Department of Education, including reading or sending e-mail and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of Orange County Department of Education Information Technology Division employees, contractors, vendors and agents with remote access privileges to Orange County Department of Education's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Orange County Department of Education.
2. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Orange County Department of Education's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Orange County Department of Education Information Technology

Division employee provide their login or e-mail password to anyone, not even family members.

3. Orange County Department of Education Information Technology Division employees and contractors with remote access privileges must ensure that their Orange County Department of Education -owned or personal computer or workstation, which is remotely connected to Orange County Department of Education's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Orange County Department of Education Information Technology Division employees and contractors with remote access privileges to Orange County Department of Education's corporate network must not use non-Orange County Department of Education e-mail accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Orange County Department of Education business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Frame Relay must meet minimum authentication requirements of DLCI standards.
7. Non-standard hardware configurations must be approved by the Orange County Department of Education's Information Technology Division.
8. All hosts that are connected to Orange County Department of Education internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Orange County Department of Education production network must obtain prior approval from the Orange County Department of Education's Information Technology Division.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel

in a frame relay network, and has local significance only to that channel.

Dial-in Modem

A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing

Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on an Orange County Department of Education provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Orange County Department of Education and an ISP, depending on packet destination.

DSL

Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay

A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN

There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access

Any access to Orange County Department of Education's corporate network through a non-Orange County Department of Education controlled network, device, or medium.

Split-tunneling

Simultaneous direct access to a non-Orange County Department of Education network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Orange County Department of Education's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Orange County Department of Education
Information Technology Division
Router Security Policy and Procedures

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the Orange County Department of Education.

2.0 Scope

All routers and switches connected to the Orange County Department of Education production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy.*

3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms **Definitions**

Production Network The “production network” is the network used in the daily business of the Orange County Department of Education. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to the Orange County Department of Education employees or impact their ability to do work.

Lab Network A “lab network” is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to the Orange County Department of Education nor affect the production network.

6.0 Revision History

Orange County Department of Education
Information Technology Division
Server Security Policy and Procedures

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the Orange County Department of Education. Effective implementation of this policy will minimize unauthorized access to the Orange County Department of Education proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by the Orange County Department of Education, and to servers registered under any the Orange County Department of Education-owned internal network domain.

This policy is specifically for equipment on the internal the Orange County Department of Education network. For secure configuration of equipment external to the Orange County Department of Education on the DMZ, refer to the *Internet DMZ Equipment Policy.*

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at the Orange County Department of Education must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by The Orange County Department of Education. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by The Orange County Department of Education.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Policy and Procedures

- Operating System configuration should be in accordance with approved The Orange

County Department of Education Policy and Procedures.

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 month.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to The Orange County Department of Education , who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within the Orange County Department of Education.
- Audits will be managed by the internal audit group or The Orange County Department of Education, in accordance with the *Audit Policy* . The Orange County Department of Education will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
DMZ	Demilitarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal the Orange County Department of Education Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

Virtual Private Network Request Form
Orange County Department of Education
Information Technology Division

All information for a Virtual Private Network (VPN) must be completed and is subject to an annual review.

District/Name
Address
City
State
Zip Code

Technical Contact:

Name
E-mail
Phone Number

Administrative Contact:

Name
E-mail
Phone

Additional Information:

Orange County Department of Education
Information Technology Division
Wireless Communication Policy and Procedures

1.0 Purpose

This policy prohibits access to Orange County Department of Education business networks via unsecured or secured wireless communication mechanisms. Wireless communication is granted only to Internet access on the Orange County Department of Education's public network.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Orange County Department of Education's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Orange County Department of Education's networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the OCDE network must be registered and approved by the Information Technology Division. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in OCDE laptop or desktop computers must be registered with the Information Technology Division.

3.2 Approved Technology

All wireless LAN access must use OCDE-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a OCDE-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History

Appendix D: Sample Job Descriptions

Central Unified School District
Sample Job Description

JOB TITLE: Administrator, Information Technology Services

SUMMARY

Under the general direction of the Superintendent, assumes primary management responsibility for the Information Technology Services Department; ensures efficient delivery of information system services and technology resources for users districtwide; and performs other essential job-related work as required. The fundamental objective of this position is to ensure that computers and technology efforts are consistent with the overriding objective of effective delivery of quality educational services for the students, parents, and community.

DUTIES AND RESPONSIBILITIES

The following are examples of duties related to this position:

1. Plans, organizes, leads, directs, develops, and monitors all aspects Services Department; supervises Educational Technology and Departments and provides direction to coordinators and supervisors of the Technology Library Services.
2. Directs and facilitates ongoing districtwide needs assessment and development of technology implementation plan to ensure delivery of efficient and effective day-to-day and ongoing information system and technology services districtwide.
3. Directs research, evaluation, assessment and testing functions, and district standardized testing program.
4. Oversees, develops, and implements the district plan for information systems and technology. Sets policy for the purchase and repair of computers, peripherals, and audiovisual equipment.
5. Directs, facilitates, and monitors information system implementation efforts to ensure that the Department keeps pace with day-to-day and future needs. Assures compliance with graduation requirements. Guides and assists departments and sites in the development of appropriate educational technology implementation and curriculum.
6. Maintains frequent group and one-on-one communication and works in a collaborative manner with department directors and other administrators and professionals districtwide to facilitate decision making and problem solving in the area of computers and technology services and assessment.
7. Oversees progress toward objectives relating to migration and other project management efforts.
8. Oversees the management of the interconnection of operating systems, desktop computer applications, network protocols, and mainframe applications.

9. Reviews, monitors, and facilitates negotiations with vendors and agencies to provide cost-effective resources in terms of day-to-day demands and longer term goals and objectives.
10. Complies with applicable state, local, and federal rules, regulations, and laws, as well as the policies and procedures of the district.
11. Establishes and maintains effective working relationships with a variety of groups, including teachers, students, administrators, coworkers, vendors, consultants, and others as required.
12. Demonstrates and models safe, prudent, and healthful work behaviors and practices; identifies and works toward the elimination of unsafe or unhealthful work area conditions.
13. Performs other essential job-related work as required.

SUPERVISORY RESPONSIBILITIES

Assign and supervise of all Information Technology Services Department employees. Carries out supervisory responsibilities in accordance with the districts policies and applicable laws. Specific requirements include, but are not limited to, the following:

1. Manages substantial data bases and other information such that the quality, quantity, time lines, and facility of data retrieval and reporting support district and site needs.
2. Manages resources so that Information Technology Services Department provides timely and essential customer service, training and user support.
3. Utilizes knowledge sufficient to manage complex data base systems, network management [LAN and WAN environment] and protocols, intranet and Internet access, mini-computer operations, and multiple hardware and software platforms.
4. Manages and directs systems that support and assist users at all sites in computer, software, network, and system functions.
5. Develops and manages long-range planning for technology, infrastructure, and network environment to facilitate technology use districtwide.
6. Manages services that provide support through multiple methodologies, including but not limited to, help desk, on site training, equipment repair, and essential data retrieval for management purposes.
7. Clearly commands knowledge and expertise sufficient to facilitate the data needed to support the district's fiscal services, business services, human resources, and student services departments and/or divisions.
8. Manage districtwide network that supports voice, video and data transmission.

QUALIFICATIONS

Education and Experience
Administrative Credential - master's degree preferred.

Evidence of successful experience and management expertise in an educational setting or similar-sized organization involving computers and technology management.

KNOWLEDGE, SKILLS, AND ABILITIES
Typical qualifying knowledge, skills, and abilities would include:

Knowledge, skills, and abilities in the area of information systems and technology resources; principles, practices, and languages used in communication oriented computer systems and programming; the capabilities, capacities, and limitations of computers and peripheral equipment; comparative equipment, planning, and cost control; principles and practices of accounting, statistics, and school district organization, activities, and requirements; principles of administration, human resource administration, departmental budgeting, supervision, and training.

Language Skills. Ability to read, analyze, and interpret common scientific and technical journals, financial reports, and legal documents. Ability to respond to common inquiries or complaints from customers, regulatory agencies, or members of the business community. Ability to write speeches and articles for publication. Ability to effectively present information to top management, public groups, and/or Governing Board.

Mathematical Skills. Ability to apply advanced mathematical concepts to resolve managerial issues and problems. Ability to understand mathematical operations for such tasks as schedules, time lines, hourly commitments, payrolls, probable outcomes, and forecasting ***I*** estimating.

Reasoning Ability. Ability to define problems, collect data, establish facts, and draw valid conclusions. Ability to interpret an extensive variety of technical instructions in mathematical or diagram form and deal with several abstract and concrete variables.

Physical Demands. The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is frequently required to walk and sit. Equal time needs to be spent observing employees job performance and accomplishments versus being assigned to only office work on an eight hour basis.

WORK ENVIRONMENT

Work is performed primarily inside an office or office/laboratory environment with occasional exposure to the elements and cleaning solvents/chemicals. Requires occasional lifting of up to 50 pounds and the full range of fingering, talking, hearing, visual, and other physical and mental work demands.

Central Unified School District
Sample Job Description

Job Title: Technical Services Director

Job Goal:
Under the general direction of the Information Technology Services (ITS) Administrator, assumes primary management responsibility for the Technical Services Department within ITS; ensures efficient management and delivery of services across the district's voice, video and data networks and performs other essential job-related work as required. Maintains the computer, telephony and communications equipment that constitute the Wide Area Network. The fundamental objective 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 information resources.

Essential Job Results:

1. Directs, develops, plans, organizes, leads, trains and monitors all aspects of the Technical Services Department and the information services they provide.
2. Directs and facilitates ongoing districtwide voice, and data communication needs and develops and implements practices, procedures, and technologies to ensure delivery of efficient and effective day-to-day use of information that fulfills the district's educational and business objectives.
3. Oversees, develops, and implements efficient support services for computer repair, network installation, desktop support, network integration and maintenance, telephony and media delivery.
4. Directs, facilitates, and monitors network services. Performs and assigns project management and ongoing support tasks to ensure the successful implementation of voice, video and data network technologies and topologies throughout their life cycles.
5. Develops and manages support activities for the following:
    - Assists Technical Services staff in providing ongoing user training to ensure efficient use of desktop systems and other end-user technologies.
    - Assists Technical Services staff in designing, distributing and presenting systemwide documentation for both users and support staff.
    - Establishes and maintains standards of security to ensure the safety of all systems and data.
    - Establishes and maintains effective procedures in setting up systemwide user accounts and the access rights each user or group is provided.
    -

- Designs, implements and monitors systems problem reporting, enhancement requests and resolution of same.
- Maintains an on-line help desk system.
- Ensures that Technical Services staff manages and monitors the district's connection to the Internet.
- Ensures ongoing support systems for the district's servers and network operating systems are maintained through application of necessary patches, upgrades and new operating systems.
- Maintains the security of the district's servers and data from virus and other electronic intrusions.

6. Manages the installation, service, repair and maintenance of the single, multi-line and electronic key telephones, electronic and hybrid key systems, and private branch exchange systems. Coordinates activities with the telephone service provider.
7. Maintains a close watch on industry techniques in software, network and project implementation methods to ensure that the department is able to keep pace with day-to-day and future needs. Incorporates this information to encourage and design effective and ongoing staff training and development.
8. Maintains frequent group and one-on-one communication and works in a collaborative manner with department directors, other administrators and professionals districtwide as well as outside agencies to facilitate design making and problem solving in the area of information technology.
9. Collaborates closely with other groups within ITS ensure their information and business needs are met by the systems the district deploys.
10. Oversees the management of the interconnection of all systems and devices connected to the district's voice, video and data networks.
11. Reviews, monitors, and facilitates negotiations with vendors and agencies to provide cost-effective resources in terms of day-to-day demands and long-term goals and objectives.
12. Complies with applicable state, local, and federal rules, regulations, and laws, as well as the policies and procedures of the district.
13. Establishes and maintains effective working relationships with a variety of groups, including teachers, students, administrators, co-workers, vendors, consultants, and others as required.
14. Demonstrates and models safe, prudent, and healthful work behaviors and practices; identifies and works toward the elimination of unsafe or unhealthful work area conditions.
15. Performs other essential job-related work as required.

Qualifications:

Education/Experience

Any combination of education and experience equivalent to a bachelor's degree from an accredited college or university in business administration, public administration, education, computer science, or related field AND eight years progressively responsible experience in a similar-sized organization in the field of computers and technology management, of which four were in a management capacity. Certified Novell Engineer or Microsoft Certified Engineer.

Knowledge/Skills:
Knowledge, skills, and abilities in the area of information technology systems and technology resources; principles, practices, and software applications; wide area networks including network operating systems, infrastructure communication equipment including switches, routers, DNS servers, Web browsers, Java; databases and programming; the capabilities, capacities, and limitations of computers and the various operating systems such as Novell, Windows-NT, Unix, desktop OS's (MacOS, Microsoft Windows, and Linux); peripheral equipment; comparative equipment; planning, cost control; principles and practices of accounting, statistics, school district organization, activities and requirements; principles of administration, human resource administration, departmental budgeting, supervision, and training.

WORKING CONDITIONS

Work is performed primarily inside an office or office/laboratory environment with occasional exposure to the elements and cleaning solvents/chemicals. Requires occasional lifting of up to 50 pounds and the full range of fingering, talking, hearing, visual, and other physical and mental work demands.

Appendix E: Study Agreement

FISCAL CRISIS AND MANAGEMENT ASSISTANCE TEAM
STUDY AGREEMENT
November 13, 2006

The FISCAL CRISIS AND MANAGEMENT ASSISTANCE TEAM (FCMAT), hereinafter referred to as the Team, and the Central Unified 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 Central Unified 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.

2. SCOPE OF THE WORK

A. Scope and Objectives of the Study

The scope and objectives of this study are to:

1) Conduct a review of the district's technology support organizational structure and staffing allocations and make recommendations for improvement.
2) Assess the district's technology support services delivery mechanism and make recommendations for improvement.
3) Assess the district's distribution of network resources and make recommendations for improvement.

B. Services and Products to be Provided

1) 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.

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

3) Progress Reports - 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.

4) 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.

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

6) Final Report - Sufficient copies of the final study report will be delivered to the District following completion of the review.

3. PROJECT PERSONNEL

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

A. Andrew Prestage, FCMAT Management Analyst
B. Greg Lindner, FCMAT Technology Consultant
C. Wade Williams, FCMAT Technology Consultant
D. Robert Chambers, FCMAT Technology 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, presenting reports, or participating in meetings.

B. All out-of-pocket expenses, including travel, meals, lodging, etc. Based on the scope of work identified in section 2 A, estimated total cost is $8,000. The District will be billed based on actual cost. Any change to the scope will affect the estimate of total cost.

C. The District will be invoiced at actual costs, with 50% due following the completion of the on-site review and the remaining 50% due upon acceptance of the final report by the District.

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 organizational charts
4) Current and four (4) prior year's audit reports
5) Any documents requested on a supplemental listing

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 District pupils. The District shall take appropriate steps to comply with EC 45125.1(c).

6. PROJECT SCHEDULE

The following schedule outlines the planned completion dates for key study milestones:

Orientation:	December 4, 2006
Staff Interviews:	December 4-5, 2006
Exit Interviews:	December 5, 2006
Preliminary Report Submitted:	January 16, 2007
Final Report Submitted:	To be determined
Board Presentation:	To be determined

7. CONTACT PERSON

Please print name of contact person: Marilou Ryder, Superintendent

Telephone 559 276-5206 FAX

Internet Address mryder@centralusd.k12.ca.us

Marilou R

Marilou Ryder, Superintendent Date
Central Unified School District

Barbara Dean Nov 13, 206

Barbara Dean, Deputy Administrative Officer Date
Fiscal Crisis and Management Assistance Team

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.