November 15, 2016

Dr. George S. Sziraki, Jr., Superintendent
Placer Union High School District
13000 New Airport Rd.
Auburn, CA 95603

Dear Superintendent Sziraki,

The purpose of this management letter is to present the findings and recommendations of the Fiscal Crisis and Management Assistance Team (FCMAT) resulting from the recent technology review. As indicated in the study agreement, dated February 1, 2016, FCMAT reviewed network infrastructure, the technology services provided by the Technology Department and technology use and support at the school sites.

The study agreement states that FCMAT will perform the following:

1. Analyze the state of the district's technology including hardware, software, and technology use. Interview principals, department directors and classified staff to gather data on the software applications and hardware used. Review the district's technology master plan with an emphasis on the integration with the Local Control and Accountability Plan (LCAP).
2. Analyze the status of the following:
    a. Infrastructure planning, deployment, and maintenance
    b. Network administration
    c. User account and password management
    d. Help desk system and ticketing process
    e. Technology related board and social media policies
    f. Hardware installation and setup
    g. Application software used at the district and school sites
    h. Technology in the classrooms

FCMAT conducted fieldwork at the district office on September 7-8, 2016, and additional off-site work during the weeks that followed. FCMAT reviewed numerous documents including board policies, equipment inventories, and network diagrams.

Overview of Technology Staffing

The district's technology is supported by eight positions in the Information Technology Department, which is led by a director of information technology who reports to the director of technology and assessment. The remaining seven positions in the department consist of site information systems administrators who are assigned to specific school sites and the district office.

Technology Plan

The most recent district technology plan is dated 07/01/2012-6/30/2015, and was developed to comply with Board Policy 0440, California Ed-Tech and federal E-Rate requirements.

Goal #2 of the Local Control and Accountability Plan (LCAP), Strengthen the Achievement of All Students Including Special Populations, developed in 2015-16, includes the following actions:

- Ensure that educators and students have access to appropriate physical and digital instructional materials and classroom supplies.
- Ensure that educators and students have appropriate technology and equipment to support digital education.

While identifying these actions in the board-approved LCAP allows for budget allocations for Chromebooks and network infrastructure under the state local control funding formula (LCFF), without a technology master plan to specify measurable objectives and timelines, progress toward the goal may be difficult to assess.

The district has developed a facilities master plan, and the board of trustees passed a resolution in June 2016 to place the Measure L general obligation bond on the local November 8, 2016 ballot to finance the plan. The proposed plan includes modernization and upgrades to classrooms and school campuses, but there is no plan to address these needs should the facilities bond measure fail.

Staff at the district and schools indicated they have focused on the 1-to-1 Chromebook (1: web) initiative since its inception in 2013, and some schools have a school site technology plan. District funds are budgeted annually to address technology needs at the schools and district level, but there is no recent, comprehensive district master plan for technology. A technology master plan would serve as a comprehensive document to gather and align the technology components mentioned in the LCAP, the facilities master plan, and the individual school site technology plans.

The 1: web initiative was driven by district leadership and has been successful in providing students with access to online resources and tools, but there is no clear, documented plan for student learning outcomes. Online curricular resources, instructional tools and tutorials are available, but in the absence of a plan that includes measurable objectives beyond the 1:1 device distribution and infrastructure capacity, there is no way to measure student success.

The district has made use of grants and an endowment fund to implement its 1: web program and improve the network infrastructure. Each school also has the opportunity to utilize these funds for its specific needs. Because there is no district plan for technology, schools have resisted efforts to centralize certain systems and procedures. One example is the uneven adoption of the centralized IT work order system.

School staff indicated their interest in retaining the independence and uniqueness of their schools and expressed concerns about central office interference and monitoring. Agreements about which systems

may be most effectively managed at the district level and which decisions are appropriately and effectively made at the site level do not exist. Without the guidance of a technology plan that is based on buy-in by all district personnel, each school defines its own objectives and strategies and there is no unified set of measurable objectives or unified purpose. New initiatives originated either at the district or schools are at risk of failure or poor outcomes.

A technology plan serves as a guiding document to articulate the district's vision for technology use, and to outline the steps and actions necessary to achieve and sustain the vision. It involves collaborative leadership to make it possible and is critical to sustaining 1:1 programs and guiding their evolution beyond the initial implementation.

Recommendations

The district should:

1. Form a district technology committee to draft a new technology plan.
2. Align the district technology plan with the facilities, administrative, and educational plans and individual site technology plans to ensure alignment and successful completion of the recommended action steps, and to optimize district resources.
3. Develop a contingency plan to address classroom and facilities needs if the bond measure fails.
4. Monitor, evaluate and update the district technology plan at regular intervals during the three-year term of the plan.

Technology Related Board and Social Media Policies

Board Policy 0440, District Technology Plan, adopted in May 2015 provides guidelines for a three-year district technology plan, but there are no associated administrative regulations. The district has no current technology master plan, although staff indicated that some components of a technology plan are included in the facilities master plan (infrastructure and modernized classrooms) and the Chromebook plan (1:1 devices and digital curriculum).

Board Policy 6163.4, Student Use of Technology, was updated in May 2015 and includes an attached acceptable use policy associated with the 1: web program. It is up to date and reflects current practice and policies regarding online safety and privacy.

Board Policies 1113, District and School Web Sites, and 1114, District Sponsored Social Media provide frameworks for school and teacher webpages and for using social media. These were adopted in May 2012 and are up to date.

Board Policy 6161, Equipment, Books and Materials, dated May 2012, refers to equipment, books, and materials for instruction but makes no specific reference to the districtwide adoption of Chromebooks and online resources for instruction. In a 1:1 environment, the administrative regulations associated with digital resources, their selection process, and access for students are recommended.

High functioning school districts update and align board policies and administrative regulations with instructional goals and vision. The process of updating policies allows the board of trustees to review and

understand emerging initiatives, and their approval and support are critical to achieving the operational and budget support needed for programs.

Recommendations

The district should:

1. Update Board Policy 0440, District Technology Plan, by adopting administrative regulations describing the technology plan process, components and planning team.
2. Update the Board Policy 6161, Equipment, Books and Materials, and administrative regulations regarding instructional materials to ensure they accurately reflect the districtwide adoption of digital resources.

Technology in the Classroom

The district adopted Google Apps for Education (GAFE) in 2009, and began an incremental 1:1 Chromebook (1: web) rollout with all sophomores in 2013. The district has now reached a 1:1 ratio for all students. Chromebook devices are distributed to each incoming freshman at the beginning of their ninth grade year that they keep until graduation. In addition to the Chromebooks, all schools have computer labs with PCs, Macs, or laptops. Classrooms have teacher computers and, depending on the class, may also contain other computers to support the specific curriculum.

When asked about the district's technology initiatives, most staff commented on the 1: web Chromebook program and the districtwide use of Google Apps for Education in the core curriculum at every school. Google Classroom, a web-based platform that allows teachers to create classes, distribute assignments, communicate with students, and organize Google docs and other student work, is used in all the schools. Students are required to take the Tech Essentials class in grade 9. There is some teacher created content in Moodle, an online, open source learning platform, which was developed by district teachers for independent study students.

Also mentioned were the Career Technical Education (CTE) program, the recent Read 180 adoption, and Moodle learning management system. Educator's Assessment Data Management System (EADMS) is used for formative assessments, report cards and data analysis.

There is a well-established practice of distance learning between district schools whereby students may enroll in classes on other campuses via Google Hangouts if there is insufficient enrollment for that class at their home school. The classes make use of large monitors and real-time connections to the off-site class using the wired network.

Information Technology staff at each site handle repairs and replacement as needed for the Chromebook program. Chromebook manufacturers are selected by a bid process that occurs in the spring in preparation for the next school year. The Chromebooks are now shipped preconfigured by the vendor to reduce workload when the district receives the devices, but the repairs on-site have resulted in a shift in workload for some school staff. Some school staff indicated that the district has made changes to the administration of the Chromebook program with insufficient notice or collaboration with the schools. Policy and program changes initiated at the district have resulted in unanticipated, last-minute shifts in workload and procedures at the schools.

All students have a GAFE account with a unique username and password. District staff manage the GAFE accounts with an automated account management system (Tools4ever) and GAFE Synch that

connects to the Aeries student information system, and the Destiny Resource Manager program is used for Chromebook checkout through the school libraries. Teachers have selected a variety of web-enabled curriculum resources suitable for their students. The schools have individually selected online tools to achieve the instructional goals for their courses. The result is a varied set of online instructional tools in the district.

As the curriculum increasingly includes technology, the demand for high-capacity, high-performing network services has increased. School staff report that the network reliability and performance have improved during the past two years, but there are some reported instances of poor wireless connectivity in classrooms and common areas.

School administrators and school site staff indicated the distance learning classes are well attended and an essential part of the scheduled offerings for students, but the facilities may not provide the quality of sound and acoustics needed for displaying online content and a consistent distance learning experience. They cited issues with aging, inadequate classroom facilities including lack of sufficient power outlets for student Chromebook charging, insufficient interactive whiteboards and projection systems, and poor sound systems and acoustics for presentations and interactive learning. Technology adoption has outpaced facilities upgrades and more updated classrooms are needed to meet the increasing use of distance learning.

Recommendations

The district should:

1. Include school site staff in planning for new procedures.
2. Consult with school site staff to diagnose and solve wireless connectivity problems in classrooms and common areas.
3. Address classroom modernization needs for upgraded power and audiovisual systems.

Application Software

At the district level in Placer Union High School District, the following applications are frequently used:

Google Apps for Education	Productivity/communications
Microsoft Office	Productivity
Escape	Financial/business system
Aeries	Student information system
SEIS	Special Education information system
AESOP	Substitute teacher calling

District staff use Gmail for district email and a combination of Microsoft Office and Google Apps for day-to-day productivity. Except for Microsoft Office, which is installed on the individual user's computer, all applications are cloud-based and hosted off-site by the vendor. Microsoft files are generally stored on the local hard drive, but some staff make use of shared folders on district servers. Staff are assigned to a single computer. They cannot access their files from other locations unless they're using Google Apps.

Many districts have shifted from a single user per computer to a network design that allows staff to log in to their files and applications from any computer on-site or off-site. The district uses Google Apps, which are accessible anywhere. Many districts have established a standard practice for document storage and retention that determines which documents are saved to permanent, shared storage on internal servers or on hosted, off-site or cloud-based locations. When required, employee files are mapped to a network drive with automatic, scheduled backups of these files. Many districts offer either a secure online location or in-house server-based storage through a secure web portal. This allows staff to take advantage of mobile devices and to access their work from any location, and ensures that critical files are saved and accessible when needed.

Escape is the district's financial/business software and is housed at the Placer County Office of Education. It includes accounts payable and receivable, benefits, budget, human resources, payroll, position control, and state and federal reporting modules. Staff stated that Escape is occasionally very slow.

In addition to the district standard applications mentioned above, the school sites utilize a variety of software and systems for varying purposes. Communications, outreach and emergency contact systems differ between sites. Systems cited by school and district staff include:

School Messenger	Auto messaging for attendance, emergencies and outreach
Remind	Attendance

Many districts adopt district-wide communications tools to ensure consistent coverage in emergencies, create efficiencies for licensing costs, training and support, and to facilitate unified messaging to families.

The district uses a variety of Voice over IP (VoIP) and analog phone systems. Some staff mentioned the lack of a school-wide public address system in classrooms. The lack of a district standard and central management for the phone and communications system prohibits district-wide messaging and call manager database support. Each system must be managed and maintained separately at the schools.

Many districts that migrate from analog to digital voice systems adopt a single telecommunications system to support unified communications, classroom safety, emergency preparedness, and to streamline E-Rate applications. Because of the critical nature of district phone systems, these projects are typically part of a facilities and IT master plan and may involve a multiyear implementation.

Recommendations

The district should:

1. Evaluate the feasibility of modifying the network design to allow all staff to access their information from any device.
2. Establish standard practices for electronic document retention and storage, and communicate these practices to employees.
3. Consult with the county office to improve the performance of the Escape system.
4. Conduct a needs assessment related to district and school communications systems and develop a plan in collaboration with school staff and administrators to select and implement a unified communications system.

Help Desk System and Ticketing Process

All IT staff track incoming requests from their respective sites and escalate them to the district IT staff as needed. IT staff also respond to email and phone requests along with online requests.

At two schools, help desk support is provided by a team of students. This improves responsiveness in those locations, but only at those sites. District and school site staff opinions about technology support response times vary widely, ranging from satisfactory to unsatisfactory. Some school site staff indicated that individual persistence is key to receiving timely technology support.

The district purchased Web Help Desk from SolarWinds for technology service and support requests with the intent to implement the system district-wide, one site at a time. Opinions vary among site and district staff about its usefulness and the extent of its adoption. Other ticketing systems in use across the district include Google Forms and TechSets/My Tech Desk.

At some schools there is resistance to a district-wide work order system. Some school staff are skeptical about the use of the data that a district-wide system may provide, and they expressed concerns that the use of an online system would detract from the personal contact and hands-on technology assistance they prefer. Some staff at both the district and the school sites indicate they receive better support by directly contacting a technician via phone or email.

There is general uncertainty among district and school staff about the extent of use of the online systems. Some school staff indicate that 85% of the technology help requests at their locations are submitted online, but some school and district staff stated that the ticketing system had been abandoned. Data from the various help desk systems are not analyzed to assess technology support requests, trends or response times.

The lack of a district-wide, standard help desk system prohibits the district and schools from knowing quantity and types of support requests, prioritizing issues for follow-up, understanding recurrent hardware, software and system issues, and quantifying needs for budget and staffing support.

High functioning districts rely on a standard, centralized help desk system in addition to on-site technicians to ensure high quality customer service, optimize technology support resources, track trends and anticipate workload. Data and reports that are available in a work order system would allow the district to analyze repair and support requests, take action to improve support systems, and contribute to the planning process by documenting needs for support staff. Also, school districts encompassing large geographic areas benefit from a central database to ensure that staff and other resources are allocated strategically, and to house a knowledge base for technicians who may not be able to meet regularly.

Successful system implementations of new help desk or other enterprise level systems include all stakeholders in the process from the beginning, and the project aligns with an overall technology master plan. Buy-in at the start lessens resistance during implementation. Timelines and training requirements are anticipated ahead of time and sufficient resources allocated to ensure successful rollout and sustainability of the system.

Recommendations

The district should:

1. Establish a centralized work order system that includes automated workflow to improve communications. Ensure that requestors have the information they need about problem resolution and projected timelines.

Infrastructure Planning, Deployment, and Maintenance

Wide Area Network Equipment and Design

The technology staff provided high-level network drawings of the wide area network (WAN) and the wireless network showing the type of connections, equipment used and contracted bandwidth. Local area network (LAN) drawings were not provided.

The district primarily uses Hewlett Packard (HP) routers and switches for the WAN and LAN and Aerohive equipment for the wireless network. The technology staff reports there is no formal written and board approved upgrade plan for the LAN and WAN equipment although there is older equipment in the network. The inventory list provided by the district shows HP switches placed into service as far back as 1999.

Technology staff reports that approximately 20 model HP1910 switches need replacement and are scheduled to be replaced this year using E-Rate funds. E-Rate is a federal program that provides discounted telecommunication services and equipment for schools and libraries. The HP switches being installed include a lifetime warranty and no additional support agreement is required. If a switch fails, technology staff will test the device and submit a support ticket to HP. If it is determined a replacement device is needed a replacement is sent to the district.

The documentation provided for the wireless network shows a centrally managed system with 254 access points throughout the district. Technology staff reports approximately 10% of the access points are outdated and are scheduled for replacement this year using E-Rate funds. Site staff reports some areas of weak coverage and they would like better guest coverage, but overall the wireless system meets their needs.

The district uses the vendor Wave to provide WAN services. The network design includes a fiber-optic cable connection from the district office to each high school. The district office is connected with fiber-optic cable to the Placer County Office of Education where the district connects to the internet. Placer School for Adults does not receive Wave services and is directly connected to Placer High School by district-owned fiber-optic cable.

The fiber-optic connections contracted from Wave are configured with a committed information rate (CIR) to meet the needs of the district office and each school site. A CIR is the amount of bandwidth a provider guarantees will be available at all times. This may be less bandwidth than the physical connection speed. It may be possible to exceed the CIR up to the connection speed if the provider's network is not busy. The chart below shows the connection speed and CIR available at each site where Wave provides service.

Site	Committed Information Rate	Connection Speed
District Office	2Gbps	10Gbps
Placer High School	500Mbps	1Gbps
Foresthill High School	300Mbps	1Gbps
Chana High School	250Mbps	1Gbps
Del Oro High School	500Mbps	1Gbps
Colfax High School	500Mbps	1Gbps

SolarWinds Network Performance Monitor is used to monitor the health and performance of the LAN and WAN. This system allows the district information systems administrator to monitor performance and potential network issues before they lead to a complete outage.

Many districts that move to a 1:1 program and use online resources will see a continual increase in bandwidth utilization. The district may also see an increase in bandwidth utilization due to the 1: web program as more online resources are utilized by students and staff. The increase in demand may quickly exceed the current CIR of the WAN connections. Many districts monitor bandwidth usage and project future bandwidth needs. This allows districts time to plan for infrastructure changes.

Technology staff reports the district does not have a documented equipment replacement plan or schedule. Individual sites may use site funds to replace older equipment or for other needs. Many districts have an equipment replacement plan so they can properly budget for network infrastructure needs. The replacement plan usually is based on the expected life cycle of specific equipment. Due to the increasing demands placed on school networks the useful life of network equipment may be less than the physical life. Several equipment vendors offer lifetime replacement of network equipment, so the hardware may still operate but it may be obsolete. It is important to consider the length of time that a specific piece of network hardware will continue to meet the needs of the district and include that in the district replacement plan.

The WAN design does not protect the district in the event of an outage on the link to the county office where the district connects to the internet. With only a single link to the internet, a failure would cause a disruption in online services to the entire district. If this occurred during the instructional day or during the CAASPP test it could cause significant disruption. An alternate connection to the internet, preferably from a different location and a different vendor, would allow the district to continue to use online resources while the primary connection is repaired.

Proper network documentation and equipment inventory will allow district staff or outside assistance to quickly isolate the source of a problem. This can reduce overall time and cost needed to resolve a network issue. This documentation will show locations of main distribution facilities (MDF) and intermediate distribution facilities (IDF) at each site. It will also show the details of the equipment used in those locations, types of connections and IP addressing in use. MDF and IDF are the physical locations where networking equipment is located. The MDF is the collection point of multiple IDF within a site.

Recommendations

The district should:

1. Consider purchasing a second internet connection for one school site to be used as an alternate path to the internet.
2. Create detailed network documentation for each school site and the district office.
3. Develop an equipment replacement plan that meets the district's needs.
4. Develop a plan for monitoring and increasing bandwidth.

Network Administration

The district information systems administrator is the primary staff member assigned to network administration. No designated staff member is assigned and trained as a backup for this position. Site staff reports they are concerned that if the administrator is unavailable their needs will not be able to be met by other technology staff members either due to lack of knowledge or lack of access to the passwords needed to maintain the equipment. Administrative password management is discussed elsewhere in this report.

As school districts rely more on network resources in the classroom it is vital to have both a primary and backup staff member assigned to network administration. Additional staff training may be needed for a backup technology staff member on the specific systems and equipment installed in the district.

Recommendations

The district should:

1. Assign a technology staff member as a backup to the district information systems administrator.
2. Provide primary and backup network administration staff adequate and ongoing professional development on the district's network equipment.

Administrative Password Management

Technology staff operates a variety of systems and applications throughout the district. Individual staff members assigned to manage a system maintain the administrative password for that system. The password is not documented or shared with other technology staff. If a staff member is not available the district may not be able to access the system functions assigned to that staff member. This may place the district in a vulnerable position in that the district may not be able to gain administrative access to systems they own.

Many districts require the administrative passwords for all systems and applications to be documented and maintained in a secure location. They review and update the documentation regularly since administrative passwords may be changed.

Recommendations

The district should:

1. Maintain a list of administrative passwords for all systems in a secure location.

Data Safeguards and Security

Firewall

The district uses a FortiGate firewall controlled by the district information systems administrator. This appliance is at the edge of the district network protecting the district from security attacks from the internet. This powerful and flexible product is widely used both in education and in private industry.

Content Filter

The district has two content filters. One is located at the district office and is a feature of the FortiGate firewall appliance. This content filter is used for all the devices that connect to the internet except for the Chromebooks. Chromebooks are filtered using Securly, a cloud-based web filtering system that will allow Chromebooks to be filtered both on and off campus.

Requests to bypass the filter are submitted to the technology department and handled by the director of technology and assessment, director of information technology and data management or district information systems administrator.

Maintaining two content filters may place additional workload on staff, requiring them to manage filtering tables on two devices.

Recommendations

The district should:

1. Evaluate the benefit and possible cost savings by moving to Securly content filtering for all devices.

Server and Data Backup

The district provided an inventory list of server hardware in use, which includes 52 servers of various makes and models. Each site is able to purchase servers as needed and the district has no hardware standards for servers. Technology staff state they base server purchases on what is the least expensive at the time. Some servers are purchased from vendors that will build a server based on user specification. Recently the district office has moved toward purchasing enterprise level equipment for more consistency in the server infrastructure. The technology staff has begun to virtualize some servers using Microsoft's Hyper-V and VMware's ESXi.. Server virtualization allows the partitioning of physical servers into multiple smaller servers. This can reduce the number of physical servers needed.

Technology staff report there is no documented backup and recovery procedure. Local server backups are completed regularly, but data stored with online services such as Google for Education are not backed up. The server backups are kept locally at each site on an ioSafe appliance. This is a network storage device that protects the data from fire and water within a disaster-proof chassis. Technology staff report that they do not keep off-site backups. This may leave the district at risk in a disaster that limits access to the server and the ioSafe appliance.

As the district continues to increase the use of technology for students and staff it is vital that services are available when they are needed. Currently if a server fails the service may be unavailable until the server is repaired or replaced. Technology staff report that the variety of servers makes it difficult to find the correct replacement parts because internal parts on some models may be different from another server of the same type.

Many districts centralize their server infrastructure and standardize on an enterprise server vendor to better manage the server farm and reduce the overall cost of hardware and management. They use virtualization software such as Microsoft's Hyper-V or VMware's ESXi to allow services to be quickly moved from a failed piece of hardware to working hardware. Many districts also centralize as many application services as possible. This allows for more consistency across the district and may reduce the downtime associated with hardware failure. With a centralized server farm there still may be a need for some local hardware at each site to handle Active Directory, Domain Name System (DNS) and print services. Active

Directory, developed by Microsoft, is a system that allows the organization to maintain a database of user accounts and passwords. This allows the system administrator to authenticate users and provide each user with appropriate access to district resources. DNS is the internet equivalent of a phone book mapping human readable alphabetic names to a computer usable numeric address. This hardware is still managed centrally, but with the Active Directory and DNS replicated locally the site still has access to local services if there is an outage on the WAN. If these services are not available locally and there is a WAN outage, the local user will not be able to log into their computers, print or get to any local documents.

It is vital to have a backup strategy that allows the district to quickly recover from a catastrophic failure. A well-designed backup system considers worst-case scenarios, runs automatically on a regular basis, and stores backup data at an off-site location. Besides basic backup and recovery of data, districts that use a virtual server environment may build a second virtual server environment at another school site or have agreements with other education agencies or vendors to share equipment so services and data can quickly be restored and run from the secondary location if the primary data center has been physically damaged. These systems are tested regularly to confirm that critical systems can be recovered within a timeframe that meets user needs.

Recommendations

The district should:

1. Evaluate the benefits of installing a virtual server environment at the district office and centralizing common services.
2. Develop district-wide standards for servers.
3. Consider moving the ioSafe backup appliance at each site to a different site to improve the backup strategy.
4. Document the backup and recovery process and assign responsibilities to appropriate technology staff.
5. Perform regular tests of the backup system to verify it meets the district's recovery needs.

User Account and Password Management

Technology staff report that user setup and management is handled differently by each site and by each application. The district uses a variety of applications that require users to be manually set up with a user account and password, and only a few systems share the user information. This may require the same user to be set up manually on multiple systems. Most but not all sites use a software tool, Tools4ever, to pull user data from the Aeries student information system to assist in setting up accounts, but it is done only at the site level for most systems. There has been some centralization of user account setup; one example is the setup process for Google for Education. Staff report it is working well.

Active Directory is managed separately at each site with independent servers. This may create a duplication of hardware and staff effort with little additional benefit to the district.

School districts deal with multiple systems that require user accounts and management. To reduce the complexity of managing multiple systems and the cost associated with account setup, many districts centralize this process. By centralizing they can establish a standard procedure and automated systems to pull data from one system and update other systems.

Many districts set up one Active Directory domain that is used across the district. They then set up an organizational unit structure that meets the district's operational and security needs. Some high school districts set up their structure by district, by school, then by user type; while others set it up by district, by user type, then by school. Either structure works well and can maintain the security needed. Districts then use available tools such as Tools4ever to pull data from their student information and human resources systems to build the Active Directory student and staff users. Using this same type of process, many districts automate this process for multiple systems, thus reducing the time needed to manage each system.

Technology staff report the district has no password complexity rules or change policy, and there is no consistency among sites on how passwords are handled. Passwords should be complex enough to make systems more difficult to compromise and should be changed regularly.

Technology staff also report that there is no practice or policy on removing access of a staff member that leaves the district. The technology staff is not notified by Human Resources when a staff member leaves or when a change is needed but is notified when a new staff account is needed. HR should notify the technology department so access can be removed or modified as appropriate when a staff member leaves the organization or changes positions.

It is vital to the security of the district's data to provide access only to appropriate users. Maintaining a current and accurate list of authorized users is important to maintaining data security. A password complexity and change policy also is essential.

Recommendations

The district should:

1. Evaluate the benefits of centralizing user account setup.
2. Centralize Active Directory with one district-wide domain with multiple organizational units to meet security and management needs.
3. Create a standardized notification process for user account creation, change and removal.
4. Create a password complexity and change policy that provides adequate security.

Hardware Installation and Setup

The district provided an inventory list of technology hardware for all its sites. Technology staff report that each site determines most of the hardware ordered and used, and is responsible for the installation and setup of that equipment. Most sites use available free software tools to assist in setup, but there is no standardized setup process for computers and laptops. There are no documented minimum standards or consistency of equipment for most district hardware. This includes the current practice of using multiple server vendors, a variety of desktop and laptop hardware vendors and types and three different phone systems.

Technology staff report they have attempted to standardize purchases of new systems by using the bid process and requiring sites to purchase items from the bid list, with limited success.

Some equipment such as routers, switches, wireless equipment and Chromebooks have been standardized across the district. Routers and switches are set up by the district information systems administrator and discussed elsewhere in this report.

The Chromebooks used for the 1: web program are ordered with a preconfiguration service. The vendor preconfigures the Chromebook to work on the school's network, allowing it to be sent to the school site without requiring the technology department to manually configure the device.

The district has begun to offer an optional Chromebook protection plan to parents that will cover damages, loss or theft of the device provided to their student. Technology staff provided the protection plan document that outlines the cost of the plan and the cost of repairs if the plan is declined.

Some districts have begun to allow students to take devices home and have struggled with how to handle devices being damaged or broken. As these devices become more than supplemental to the educational process it becomes unclear if the district can request parents to pay for unintentional damage. Some districts have requested parents donate a small fee toward a self-insured repair plan offered by the district, while some feel they can only charge for intentional acts of damage.

As school districts rely more on the use of technology it is vital to have standardized equipment and setup procedures that can meet district needs. Many districts develop equipment standards that all sites are required to follow. This may include selecting a limited number of enterprise-level vendors that can provide ongoing support with available replacement parts. By doing this, a small inventory of spare parts can be maintained locally and all technology staff can be trained on the specific equipment used. In addition, staff can be trained on the use of common tools and setup procedures. This may provide better overall technology support to the district by allowing technicians to assist each other as needed and back up a technician that is out of the office.

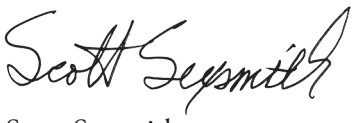
Recommendations

The district should:

1. Develop district-wide standards for end user devices.
2. Evaluate standardizing on common software setup tools.
3. Provide ongoing training for technology staff on the selected tools and setup procedures.
4. Review the Student Chromebook Protection Plan & Notification document to make sure it meets local and state requirements.

FCMAT appreciates the opportunity to serve the Placer Union High School District and extends thanks to its staff for their assistance during this review.

Sincerely,



Scott Sexsmith
Management Analyst