



West Valley - Mission

Community College District

Technology Plan for 2022-2025

Update for 2024

Contents

- Introduction..... 3
- Technology impact..... 5
- Policies governing technology. 5
- IT department structure 6
- Service and support..... 7
- Equipment lifecycle and refresh process..... 10
- Department functions 11
- Accreditation findings..... 14
- IS assessment survey 16
- Information Systems projects..... 20
- Technology goals and strategies..... 20
- Technology consolidation 21
- Educational Technology Services..... 21
- ETS impact on strategy for Students 23
- Appendix A: Fresh Service statistics 24
- Appendix B: IT Department organization chart..... 25
- Appendix C: NIST Cybersecurity Framework analysis..... 26
- Appendix D: Equipment Lifecycle & replacement plan 31
- Appendix E: IT Fixed Cost allocation 2023 -24..... 32
- Appendix F: External Wireless heat map for West Valley College 33
- Appendix G: External Wireless heat map for Mission College 34
- Appendix H: 2022-2023 Accomplishments..... 35
- Appendix I: 2024- 2025 Goals and objectives 36

Introduction

The purpose of the West Valley Mission Community College District (WVMCCD) Technology plan is to address district-wide technology, support, and resource planning to further the mission, vision, and strategic direction of West Valley College and Mission College. The plan is linked with other institutional plans and program reviews for instruction, student services, and administration. The Technology plan differs from the College Technology plans in that the former focuses on district-wide resources, policies, and strategies and the latter focuses on instructional and academic resources, procedures, and operations. When there are areas of overlap between the two areas, those linkages will be documented. This document was written by the Technology department and in addition to being a snapshot in time from an operational perspective, the objective of this document is to provide a vision for technology covering the years starting 2022 through 2025. [The Information Technology \(IT\) department consists of two primary areas: Information Systems \(IS\) and Educational Technology Services \(ETS\). The IT department has two primary roles: to support operational requirements and to plan, develop, and deliver technology projects and services. Since technology is constantly changing, the goal is to review and update this document as often as possible.](#)

Information Technology mission

The mission of the IT department is to build a solid comprehensive technology infrastructure; maintain an effective and operational environment and deliver high-quality information services that support the colleges programs for instruction, research, student services, and administration.

Background

The West Valley-Mission Community College District is comprised of two higher education institutions including West Valley College in Saratoga and Mission College in Santa Clara. The District Office is located on the West Valley campus. Each semester students take in-person courses at the colleges, while others take online, off-campus, or non-credit courses offered through a variety of instructional programs. Technology is an integral component of multiple aspects of learning, teaching, and student support as well as the foundation and infrastructure for administrative and business processing. Given its broad perspective among different groups, technology is utilized in many contrasting ways. Students utilize technology to apply to either college, register for classes, and complete coursework. Faculty use technology to develop curriculum, obtain class rosters, input course grades, and provide a distance-learning environment. District and college staff utilize technology for accounting, scheduling classes, managing student data, communicating, and managing their daily work. Strategically, technology is used for data reporting and statistical analysis to support institutional planning and decision-making.

Technology planning

This technology plan serves to fulfill the mission of providing current and emerging technology, to achieve compliance with accreditation and regulatory standards, and to evaluate and develop future initiatives and projects. During the planning cycle the IT department assesses departmental functionality, and quickly identifies areas for improvement. The Accrediting Commission for Community and Junior Colleges (ACCJC) influences the content of the IT department plan and methods to improve institutional effectiveness. The ACCJC Standard IIIC, Technology Resources, covers the areas of technology services, support, infrastructure, systems, computer hardware, and computer software. The goal is to ensure that these areas are appropriate and adequate to support the institution's management and operational

functions, academic programs, teaching and learning operations, and support services. It further states that each institution is responsible to continuously plan for, updates, and replaces technology to ensure its technological infrastructure, quality and capacity are adequate to support its mission, operations, programs, and services.

Planning process

The requirements assessment is the first step in the technology planning cycle. The goal is to establish or evaluate where gaps may exist or to evaluate the effectiveness of the service or resource. This information should be documented to support a plan for improvement. Once stakeholder communication is sufficient in addressing those needs, staff resources should be developed. This is an opportunity to determine and establish the skillsets needed as well as training requirements. As the development phase begins, a test environment should be established if possible. This step will help to improve the quality of the final product, which culminates with project implementation. See the diagram below for a visual reference.



Sustainability

When evaluating the sustainability of technology, several key factors are considered:

- Technology changes rapidly, as often as every 12 to 18 months.
- Trends and emerging technologies are evaluated for effectiveness, support, and affordability.
- Staffing Resources needed to maintain and support technology must be included in the plan.

- Technology is a key element in both institutional and educational strategies, but it is not the entire solution. Infrastructure impact and cost should be analyzed as part of an overall technology plan for the district and colleges.

Technology impact

The district leverages technology to support its mission to deliver enhanced learning environments, support systems, and quality instruction. These technologies provide educational opportunities, personalized student services, and effective administrative processes which meet the needs of the colleges and their communities.

Technology is a broad subject that applies to many aspects of teaching, learning, research, communication, and operations at each college. Such technologies are typically categorized as instructional technology or administrative technology. The former is associated with academic resources for teaching and learning, the latter is associated with administrative resources for communication and operations. These technologies include computers, servers, software, databases, printers, networks, applications, storage devices, video projectors, video conferencing, and many other types of equipment. Many technologies are used for both instructional and administrative purposes. Due to this overlap, it is necessary for the Technology Plan to address both administrative and instructional technologies.

Some technologies at the colleges are more specific to academic or vocational courses, such as, electronic music keyboards, microscopes, and spectrometers. These technologies are specialized instruments or tools that are discipline-specific or industry-specific. Faculty members may consult with both internal and external advisory councils to ensure the use of relevant technologies in their programs. Furthermore, instructional programs engage in Program Review cycles to evaluate the effectiveness of the deployment and to develop plans. Program Review plans are tied to resource allocation processes that provide an avenue of funding for specialized technologies.

This Technology Plan is focused on planning administrative and educational information technology resources and infrastructure that have a broad application across the colleges. The technology plan addresses how technology resources will be implemented to further the mission of the district and improve institutional effectiveness. This plan does not go so far as to specify the details of all the specialized technologies that would be included in program reviews; that is left to the subject matter experts. However, the Technology Plan addresses how specialized technologies will be integrated within the district technology infrastructure and ultimately enhance the support services of the colleges.

Policies governing technology

The guiding principles and strategies for using technology at the district can be found in Board Policies. BP 3720 (Computer and Network use) can be found on the main district website under the following link: [WVM Board Policy Chapter 3](#). The companion Procedure AP 3720 (Information Technology Use) can be found at the following link: [Information Technology Use](#). Additionally, BP 3721 (Information Security) was approved on 5/17/22 and is found: [BP 3721 Information Security on Boarddocs](#). The companion procedure AP 3721 (Information Security) can be found at [AP 3721 on External Tech Docs](#). The document calls out the need for a district Information Security Program Plan which has been

documented with the [Cybersecurity plan dated 4/5/2022](#). Since that time, the National Institute of Technology Standards (NIST) Cybersecurity Framework has been added to Appendix C in this document.

IT department structure

The Information Technology management team includes the Vice Chancellor Information and Educational Technology, Director of IT Applications, Director of IT Operations, and Director of Educational Technology Services.

Several task teams have been designed to coordinate technology-based discussions and requirements with staff who have a vested interest in decisions that are made related to technology. This includes staff working in technology as well as with others throughout the district:

1. The Change Advisory Board (CAB) consists of over 15 server, network, support, and management staff among Applications, Operations, and ETS groups who meet bi-weekly to discuss any impacts or projects related to the district resources.
2. The Accessibility (ADA) group consists of technology staff related to accessibility support as well as several dozen staff and faculty from both Colleges in the areas of Disability Support Services and Instruction meet monthly to discuss accessibility items districtwide, legal precedent, and to collaborate on effective solutions that meet instructional needs for students and administrative computing needs for staff. One of the goals of the group has been to define a process for review and approval of Voluntary Product Accessibility Templates (VPAT).
3. The Technology Advisory Coordination (TAC) team consists of the IT Managers, IT Architects, and the Vice Presidents of Administrative Services from each College. This group meets monthly to discuss technology-related decisions with the resulting fiscal and technical impacts.

The Technology Department has three major components or service centers. First is the Operations area where maintenance, service, and support are the key aspects. The Applications group is the second primary area where the delivery of new or updated technology opportunities for the district takes place. The last area is the Education Technology Services (ETS) group where all aspects of Instructional or Academic technology is provided. Each of the areas provides both service and support along with project management. [The organization chart and department structure can be viewed in Appendix B: IT Department Organization chart.](#)

Applications Team

The IS Applications group contains the Banner team and the Web team. They provide daily technical support to all modules in Banner including Degree Works, Banner Document Management (BDM), Banner Communication Management (BCM), develop ancillary Banner application modules and builds Banner integration with over twenty third-party vendors. The Banner team is responsible for submitting term-end annual MIS reports to the State Chancellor office, data for the National Student Clearinghouse and 1098-T tax information. Additionally, they provide internal institutional reports to users across the district and external reports to other agencies using the Argos reporting tool, PL/SQL scripts, Microsoft Power BI, website development, Banner security, and cybersecurity. In 2020 a new organization structure was developed and staff implemented the following projects:

- AwardSpring (Scholarships)
- CALSTRS reporting

- COVID-19 vaccine card image capture & status survey
- Cranium Café (Student Appointments)
- eLumen (Curriculum and assessment management system)
- Faculty load data page
- Faculty load sheet
- Handshake (recruiting platform)
- Mission College MyPhoto
- Non-credit student application

Operations Team

IS Operations group consists of the client support team, the server team, and the network team. The client support team is responsible for management and support of printers, the refresh and provisioning of computers, helpdesk support, VDI, and student workers. The network team manages wired and wireless networks, routing and switching, Virtual Private Networks (VPN) to Ellucian and the cloud, campus firewalls, public internet, datacenter management, VOIP telecommunications, and network monitoring.

Recently the Operations group has implemented multi-factor authentication districtwide in a four-part deployment plan during 2021 starting in August to improve Cybersecurity. They manage identity management, ADAP functionality connectivity with Banner, Microsoft Office 365 administration, SSO and other third-party interfaces. New computers and printers were purchased and deployed to replace aging hardware at both the colleges and the district. Two additional student workers have been hired and trained at the helpdesk to augment help desk support availability and incident ticket response time.

[The ETS team is covered in more detail on page 21 of this document.](#)

New Organization Structure

A new hierarchy of leadership allowed the department to restructure the roles and responsibilities of its support teams and add a new position for each group: Principal IT Architects. These high-level IT positions architects serve in leadership roles as they provide Project Management, supervision, and direction for other team members. [It's also important to point out that the IT department has designed a Student Worker technology program to develop their knowledge and skills. In addition to supporting the half dozen students who are engaged in the program, the IT department gains a valuable and effective resource providing service and support for the technology needs of faculty and staff at the district.](#)

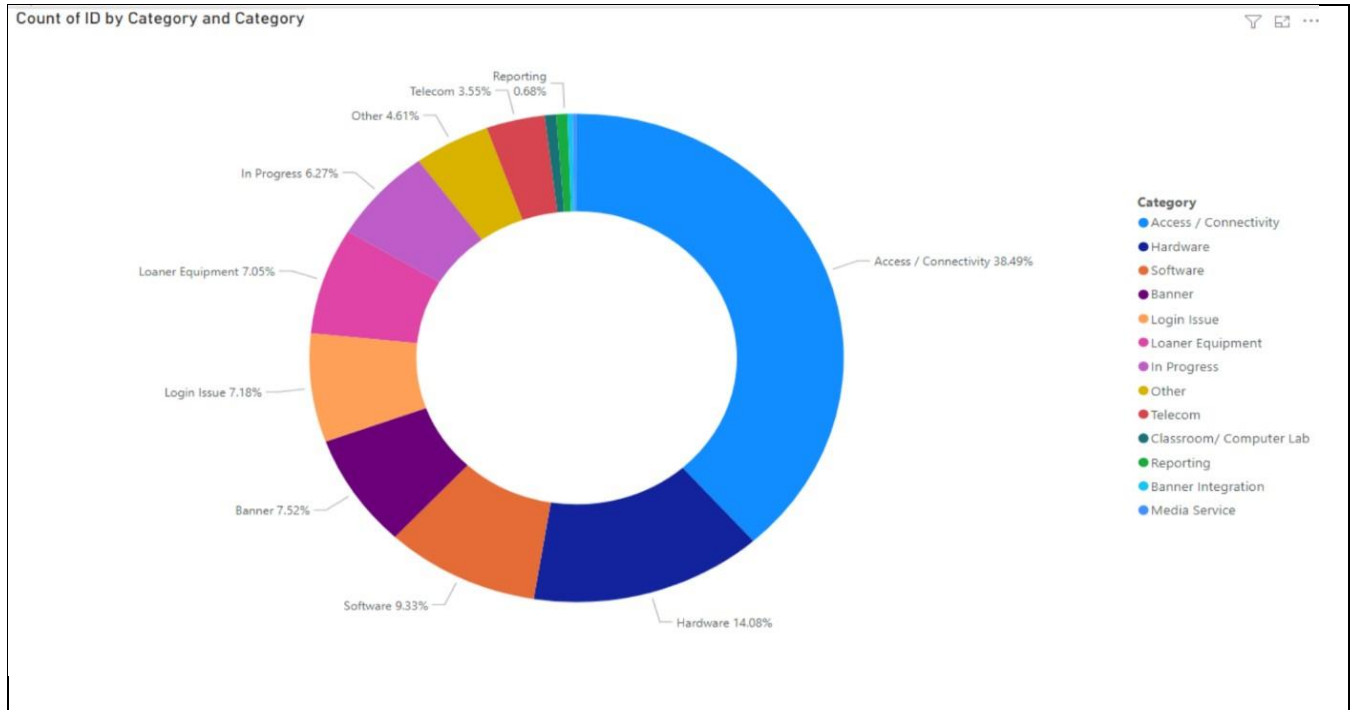
Service and support

The cornerstone of a strong technology department is the delivery of good service and support. This area is critical because high quality and timely service and support can provide efficiency and effectiveness for an entire organization whereas poor service and support can cripple an organization. Besides the need to improve the level of technical expertise in some areas, the strategy and ability to communicate with the user community needed to be improved. Lastly, the timeliness or responsiveness when the support was provided was addressed. Like many things in the technology field, a process needed to be developed using industry standard tools. To achieve these goals, a district-wide service management system, known as Fresh Service, was implemented.

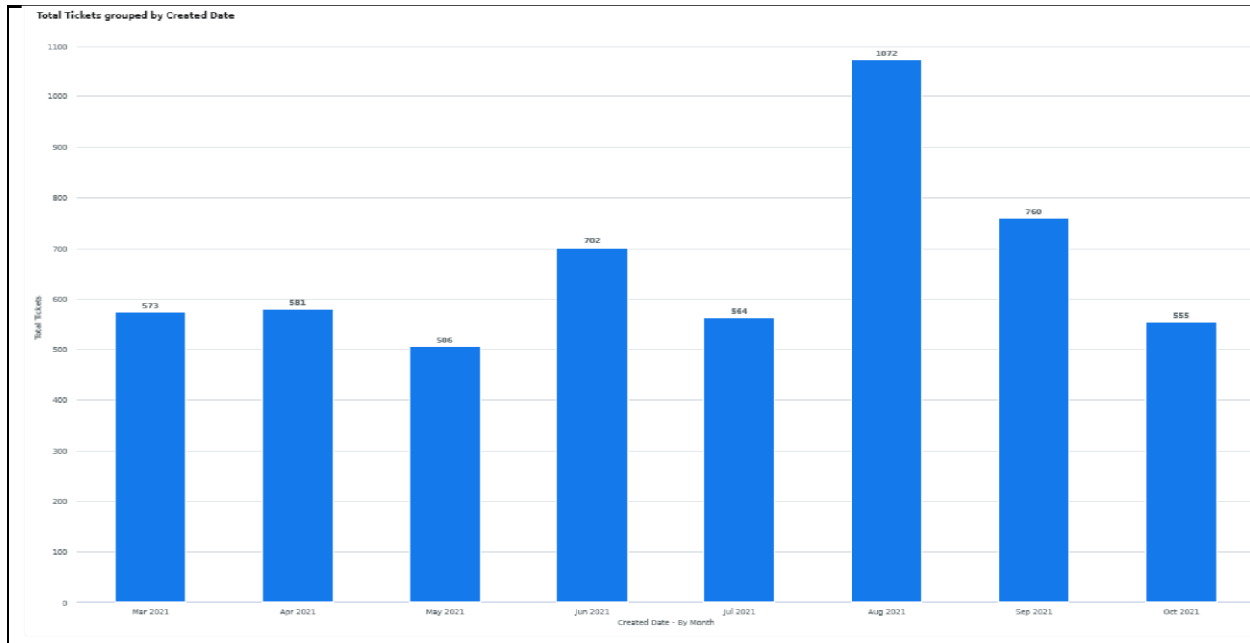
Service management system

All client service areas were addressed with the newly implemented service management system. Fresh Service was officially launched districtwide in the Spring of 2021. It was built and designed to impact all support areas for students, staff, and faculty alike. Besides providing a single source for support and better information with enhanced user communication, the system also helped to deliver statistics that has allowed the IS management team to monitor and track individual requests.

The following chart shows the different types of requests that are being maintained in the system. One can see that Access/Connectivity requests comprise the largest percentage of all tickets that have been entered into the system:



The next chart shows how many tickets have been processed in the system since it was implemented in from March – October in 2021:



It can be noted that although the average number of tickets each month was about 600, there was a large spike in August where over 1000 tickets were processed. This was related to the start of the Fall semester. Several different service desk tools were included with the Fresh Service core system including incident ticketing, workflow automation, service catalog, knowledgebase, mobile app, and improved alerting and notification.

[Appendix A](#) was created to show the Fresh Service Ticket numbers from March 2021 to October 2021. This information has since been updated by adding the information for 2022 and 2023.

When the system was first implemented Information Technology was not centralized in one department. From a user support perspective, it was important to provide simplified access to the three technology support organizations across the district. These include, West Valley Academic Technology, Mission College Educational Technology Services (ETS), and District Information Systems. By placing these three support organizations in the same service desk system, it has allowed the teams to better collaborate and deliver high-quality technology service and support. This became a moot point when both departments merged into one technology organization.

Through Fresh Service web portals end users can submit incident tickets for technical issues, or service catalog requests for common software and hardware items. As different support teams provide service on user's tickets, users receive notifications and communication from the system as their request is processed through to completion. With all support teams on a shared system, this environment has allowed cross-functional technical staff to collaborate and resolve issues with greater efficiency. The Fresh Service implementation has resulted in increased effectiveness of incident ticket routing, enhanced alerts and notifications, greater accountability, in-depth reporting, and analytics. Having oversight into the incident ticketing system has significantly helped improved response times and accountability of requests received. Additionally, the Fresh Service implementation has allowed the IT department to consolidate

two prior open-source ticketing systems that were running OS Ticket for the colleges into a single system. The IT department has improved service due in some part to the implementation of Fresh Service.

In addition to using the Fresh Service management portal for all technology requirements, the system grew in 2022 and 2023. It has become a district standard for service management by incorporating Facilities Operations and both Institutional Research and Marketing departments from each College. The next plan on the horizon is to include Human Resources as well.

End user documentation

IT facilitated the creation of significant end user documentation. This documentation covers frequently used applications, access methods and technology including multi-factor authentication (MFA) setup, VOIP telecommunications, Office 365, email configuration, Zoom, VDI setup, single sign on (SSO), and the use of Microsoft Teams and SharePoint. These end user support documents are published online and accessible to all district staff.

Client support

IT currently supports staff and faculty desktop and laptop computers that are district owned. These computers are distributed between each campus and the district office. IT specifies, configures, installs, and supports computers for employee positions as well as maintains a technology refresh program for aging computers and printers. Each scheduled technology upgrade is based on emerging technology standards.

Phone support

The Phone system was recently enhanced where the Helpdesk phone support structure was changed from the traditional one-person phone to a true call center. The original configuration would route calls to one person, and voicemail thereafter resulting in users waiting for a return phone call. With the reconfiguration of the inbound call routing from one person to a call center setup, a multi-personnel support model has been established resulting in decreased waiting times and increased live person phone support. This change also provides the means for student workers to connect to the call center pool and grants the capability for multiple individuals to provide phone support simultaneously. This change brings additional benefits and information through reports and analytics. It also provides accountability through tangible data and reports.

Equipment lifecycle and refresh process

The equipment refresh strategy addresses the need for ongoing technology equipment replacement. The district manages over 1,100 computers between both colleges and the district. Aging computers are replaced with new equipment to ensure satisfaction of the business requirements for those who use them. The computing infrastructure within the district and the colleges is comprised of hundreds of devices including desktop and laptop computers, monitors, and printers. Over time these resources become obsolete causing performance issues, repeated support and repair activity, Cybersecurity vulnerabilities, and the loss of reliability. To manage these impacts, an equipment upgrade and replacement program has been implemented.

Currently, the district evaluates active computer inventory five years or older for a potential replacement. At the start of a rotation, active inventory reports are built that show the relative ages of production computers. This data allows the district to determine where to allocate resources for computer

replacement. With this data the district determines current requirements compared to established district standards. District computer standards are posted in the WVM web portal, and they are reviewed and updated annually. Standards are provided for common desktop and laptop computer configurations.

From 2020 -2021, the IT department has deployed 550 new computers. Starting Fall 2020 and continuing through the Summer of 2021, IT replaced (200) full-time faculty laptops and (100) desktops for staff that met the established replacement criteria. IT also managed all aspects of implementing these new desktops and laptops including receiving, configuration, deployment, and subsequent disposal of all surplus hardware in compliance with the board policy and procedure regarding surplus (AP6550). During Spring 2021, a total of 150 desktop computers were ordered and deployed through a one-time COVID-19 budget allocation. These computers were distributed evenly between the district and two colleges at 50 each. Here is a summary of what was deployed to staff and faculty.

Quarter	Computer	Quantity
Spring 2020	Desktops	50
Spring 2020	Laptops	200
Summer/Fall 2020	Desktops	100
Spring 2021	Desktops	150
Spring 2021	Laptops and Desktops	50

The benefits of these recent computer refreshments include providing new equipment for faculty and staff members to run modern software and applications more efficiently. Other benefits include:

- **Cost Reduction** through greatly reduced frequency of repairs and troubleshooting for older equipment.
- **Solving Problems** associated with older operating systems no longer being supported, along with a lack of security updates.
- **Equipment Failures** addressing the risk of total equipment failure.
- **Systems Management** allows the department to move to Microsoft’s fully supported latest operating systems and ensure critical security patching routines through Microsoft System Center Configuration Manager (SCCM).

[In addition to a structured user computer replacement plan mentioned above, the IT department developed a comprehensive Equipment Lifecycle & replacement plan in 2023 for all technology equipment by adding all AV equipment, network infrastructure, and servers. This information has been documented in Appendix D: Equipment Lifecycle & replacement plan.](#)

Department functions

Within the IS group there are two technology support teams: Applications and Operations. Each team provides support for different components of district technology. The Operations group supports administrative desktop computing, network infrastructure, district datacenters, telecommunications, and Cybersecurity. The Applications team provides daily support for Banner, implementing and maintaining Banner 3rd party interfaces, server infrastructure, Institutional, State, and Federal reporting, district website, single sign on, email accounts, and user access.

Administrative Computing

The IS department manages and maintains all technology services through a hybrid physical and virtual server environment. During 2020, Information Systems has consolidated its aging physical and virtual servers into fewer numbers by upgrading the VMware virtualization environment and the hardware that it lives on. The district will continue to invest in the expansion of VMware Enterprise server and desktop virtualization. This will involve leveraging the new infrastructure to handle rapid technological change including system upgrades, testing, and implementing new services rapidly. Additionally, it will involve integrating both Disaster Recovery (DR) and High Availability (HA) features in both the server and desktop virtualization environments.

To effectively manage the datacenter technology life cycle, the Principal IT Architect of Operations has been designated as the datacenter owner. As the datacenter owner, it is the Principal IT Architect's responsibility to provide oversight into current datacenter operations, maintenance, and planning. Through designating a datacenter owner, the district has achieved comprehensive management of centralized computing resources.

Network Infrastructure

The district provides an extensive modern network that allows access by district staff and college faculty and students. The network comprised of an enterprise style infrastructure with two distinct campuses connected by a WAN circuit. The Corporation for Educational Network Initiatives in California (CENIC) provides two 10Gb network circuits. A primary circuit from Oakland for both colleges, and a secondary or backup circuit from Sunnyvale that becomes active should the primary circuit fail.

District Datacenters are located at each college campus, with the primary datacenter at West Valley college. These datacenters contain physical servers, storage, network switching and routing equipment, firewalls, and voice over IP switches for the campus phone systems. Each datacenter has an emergency backup generator and datacenter sized UPS system.

- **Wireless Network Infrastructure** is increasingly important as mobile devices and laptop computers are utilized by faculty, staff, and students. Access to secure wireless networks will continue to expand in public areas, academic classrooms, buildings, and other venues, such as the library, athletic fields, and administrative areas.
- **Network Cabling Standards** CommScope standards are utilized district wide in all administrative and instructional areas. This standard specifies physical components and installation methods for a generic telecommunication cabling system that will support a multi-product, multi-vendor environment.
- **Network Management** Infoblox provides infrastructure management of DNS, DHCP and IP Addresses. These network services assign and resolve IP addresses to systems and applications in a TCP/IP network.
- **Telecommunications** WVMCCD runs a modern district wide phone system that utilizes voice over IP (VOIP). This phone system provides service across the district which includes four-digit dialing, voicemail, campus phone directories, software phone functionality, and remote off campus access. This Mitel system supports selected analog and IP connectivity for extended uptime in case of a prolonged power outage.

Server Infrastructure

- **Servers and Storage** The district has deployed HP Synergy servers and Nimble storage in two distinct storage area network environments. These environments provide the district and the colleges with enhanced virtualized environments for running servers.
- **Data Recovery** The district utilizes CommVault for backing up servers, applications, and databases. The purpose of this backup infrastructure is to minimize the operational and financial impact of a server, application, or total system failure. CommVault provides for disaster recovery and efficient management of recovery tiers and backups.
- **Enterprise Resource Planning (ERP)** The district began implementation of Ellucian Banner in 2016. Banner is a fully integrated ERP application system that supports Student Modules, Financial Aid, Finance, Procurement, Human Resources, and Payroll. These modules leverage comprehensive data to improve departmental workflows, business processes, productivity, and efficiency for the district and colleges. Ellucian Banner is comprised of several on premise servers that provide 24/7 access to Banner in the Cloud for Internet Native and Self-Service Banner. The Banner implementation is hosted entirely in the cloud.
- **Business Intelligence** Argos is a business intelligence tool designed to support reporting institutional data. It is integrated with Banner and allows for standardized, custom, and ad-hoc reports to be created.
- **Cloud Operations** Cloud-based applications are a significant part of the administrative computing infrastructure. Ellucian Banner and Microsoft Office 365 are both cloud-based systems that have facilitated remote connectivity that has been required during the pandemic.
- **Microsoft Office 365** is a cloud-based service that provides a variety of Microsoft applications such as Word, Excel, PowerPoint, Outlook, OneDrive, and Teams for sharing and collaboration. Microsoft Office 365 is made available to all students, staff, and faculty districtwide.
- **Directory Services** Core administrative servers in the district utilize Microsoft's Active Directory (AD) identity management system. Administrators have access to centralized user provisioning and rights management as well as control over computer and user configurations through active directory functionality. AD is an industry standard identity management and directory service platform. Active Directory is extended to Microsoft Azure which provides cloud capabilities for the district and supports email along with collaboration services through Office 365.
- **System Center Configuration Manager (SCCM)** District Information Systems also deployed System Center Configuration Manager. This systems management platform provides complete software lifecycle management of district servers, desktops, and laptops. It allows the team to patch systems efficiently and effectively and achieve compliance regarding Cybersecurity. SCCM provides further management insight through data, reporting, and analytics of the devices supported by the IS department.

Cybersecurity

WVMCCD recognizes the importance of Cybersecurity as a component of planning and supporting the continuity of its technology infrastructure. The district datacenter is treated no differently than other data centers when planning for uptime and preventing possible disruption. The Principal IT Architect of Applications is the dedicated owner of Cybersecurity for the district. Here are some recent Cybersecurity initiatives that were implemented.

- Multi-Factor Authentication has been implemented for enhanced end user security.
- Malicious Domain Blocking and Reporting
- Security Incident Event Management (SIEM) is in place to reduce threats and minimize vulnerabilities.
- KnowBe4 (phishing campaign processing system)
-

The Cybersecurity environment has been hardened extensively in 2022 and 2023. The number of threats that exist on the Internet have grown exponentially. With that in mind the Information Technology department has set up a Security Operations Center (SOC) to help organize and deliver a strongly protected environment for technology. Documentation based on an industry standard framework summarizes the Cybersecurity posture at WVM can be viewed in Appendix B: NIST Cybersecurity Framework.

DNS and IP management

The IS group identified the need to upgrade an existing core network infrastructure system called Infoblox. Infoblox provides network IP address management through industry standard DNS and DHCP functionality. When the upgrade was completed, this new system provided the district with a new IP Address Management (IPAM) infrastructure as well as providing service and value for students, staff, and faculty. Infoblox provided several new appliances and servers. The new Infoblox system provides enhanced core network functionality so that WVM servers, systems and applications can connect to internal or external resources.

Accreditation findings

The Accrediting Commission for Community and Junior Colleges (ACCJC) influences the content of the district plan and evaluation steps taken to improve institutional effectiveness. The ACCJC Standard III-C, Technology Resources states that technology services, professional support, facilities, hardware, and software are appropriate and adequate to support the institutions management and operational functions, academic programs, teaching and learning, and support services. It further states that the institution continuously plans for, updates, and replaces technology to ensure its technological infrastructure, quality and capacity are adequate to support its mission, operations, programs, and services. Typically, a response from an accreditation team drives the technology planning. This section will address the ACCJC accreditation visiting team’s findings during the last evaluation in Spring 2020. To improve quality and ensure that the capacity of technology is adequate to support the College’s mission, operations, instructional programs and services, the district should continuously plan and coordinate technology refresh cycles and replacements with the colleges.

The District’s Information Systems department has completed several planned changes regarding departmental operations in relation to developing a better and more cohesive connection for both Colleges, technology planning, and technology implementation.

The following items correspond with the findings listed in the Accreditation Response Plan ‘III.C.2.1-1_IS Accreditation Response’. Each of the following items presented by the Accreditation visiting team have been addressed and a description of successful outcomes for each is detailed below.

Helpdesk Processes and Support

Both Account and Helpdesk processes need to be streamlined to meet the requirement of supporting students with improved accounts and email services.

Results:

- The district implemented a new service and support system called Fresh Service. This system brought together technical support operations districtwide.
- To provide enhanced support availability, calls are now routed to a newly established IS department helpdesk call center. This change has increased efficiency of calls answered and decreased the number of end users sent to voicemail. It is also possible to view analytics, metrics, and metadata from the Mitel call center which is useful for understanding current support needs and identifying patterns in support requests.
- Account privileges and licensing through Microsoft Azure have been optimized to provide the best possible tools, resources, and experience through Office 365. This has increased the available number of seats for high-level licenses.

Communication and Collaboration

The need for a formal meeting between the colleges and district to discuss technology, needs assessment and planning was identified.

Results:

- The Technology Advisory Coordination (TAC) team was created to improve connections between entities. The TAC provides collaboration and enhanced communication between both colleges and the district. The current structure and membership of the TAC is as follows:

Position	Area
VC, Technology, District	Information Technology Department
IT Director, Operations	IS- Client Services & Network
IT Director, Applications	IS – Applications
IT Director, Educational Technology Services	Educational Technology Servies
Principal IT Architect, Applications and Cybersecurity	IS – Applications
Principal IT Architect, Network infrastructure	IS – Operations
Principal IT Architect, Academic applications	Educational Technology Servies
Sr. IT Analyst	Educational Technology Servies
MC VP Admin Services	Mission Admin Services
WVC VP Admin Services	West Valley Admin Services

- TAC Meetings have become an integral part of reviewing action items, technology projects, and implementation plans that align both colleges and the district while progressing toward achieving common goals and strategic initiatives.
- The Technology Advisory Committee also performs a procedure for vetting new software purchases. The Software Application Request (SAR) process is built into a Fresh Service workflow automation that collects all the information needed to evaluate new software.
- **Information Systems Fixed Costs** District Information Systems consolidated all software and hardware purchases for the three entities in a process determined by each college Chief Business Officer (CBO). All three organizations were aware and advised about this change. Due to this consolidation fixed costs for technology are now centralized with District Information Systems. Fixed costs are reviewed against current costs annually by each Director and the Associate Vice Chancellor in consultation with campus Chief Business Officers. This ongoing budgetary review allows for input from the campuses based on subjective needs. This change has provided the district with financial insight and the ability to reasonably anticipate future software licensing and hardware needs.

[The annual Fixed Cost allocation for Technology can be viewed in Appendix E: IT Fixed Cost Allocation](#)

District IS Staff Training

In January 2022, District Information systems started a new Enterprise Learning subscription training program with VMware. This program will provide technical support staff with valuable training on various VMware virtualization products including VSphere, Virtual Desktop Infrastructure, and NSX. This structured training content will enable District IS staff to keep their technical skills up to date and to maintain existing systems running VMWare products effectively. It will also allow District IS to execute new projects that utilize emerging technologies like VMware NSX and site to site communications.

IS assessment survey

A districtwide IT Assessment survey was prepared and sent to all constituents across the district with the purpose of evaluating the performance, uptime, and efficacy of Technology support. Survey questions and data points were carefully selected to provide the highest insight into improvement opportunities.

The survey was sent out to a total of 1276 districtwide employees via email for responses over three weeks from November 8 through November 29, 2021. Of the 1276 employees surveyed, we received 189 responses in total, which represents a 14% response rate. A total of seven questions were part of the survey to assess and measure service and support from the Applications, Network Infrastructure, and Client support teams. The final two questions were configured to allow open responses addressing the current needs for end user training and suggestions from the end user perspective on how we can improve overall service and support.

A significant amount of positive feedback from end users was received. Some of the feedback acknowledged the contributions of individual team members. There was also feedback that expressed

gratitude for the entire department. Here are some sample comments taken directly from the survey data:

"I am extremely thankful for all of the help that Christina Chu provides to the Financial Aid Offices."

"Luis - thank you for all the hard work you put in daily and quick response!"

"I am very happy with the Information Systems Desktop technicians. Jim and Quang are always responsive and try their very best to resolve the problem quickly and without disruption."

"The District Information Systems team is very professional and provides excellent support services." "

"I have had an excellent experience with IS support staff. They have always responded very quickly to my questions. I would like to commend all of you for your skills and your awesome people skills. Could not think of a better team to support me. Thank you."

For the two open ended questions in the survey, these were the areas and items that those surveyed requested most:

Over the course of the previous two years, each of the following items that were indicated in the survey showed some level of improvement which has been indicated in a blue font:

- Improve customer service throughout District Information Systems
 - ✓ This topic has seen steady improvement in two primary areas: Service management using Fresh Service has taken off and delivered big benefits and the newly hired IT staff gained significant knowledge and experience which resulted in improved customer service.
- More transparency over which specific support staff work on various requests.
 - ✓ The Tech plan itself helped with this endeavor by documenting all IT staff and the various areas of responsibility. In addition, significant projects have been discussed in the same document.
- Enhance and improve Wireless network coverage and capacity.
 - ✓ This was one of the more strategic and extensive projects that the Network team completed in late 2023. At the cost of \$1.3 million dollars, all previous wireless access points were replaced (primarily internal) and another 100 external access points were deployed. The heat maps showing the new wireless signals can be seen in Appendix E: External Wireless heat map where there is one map per campus.
- Hire more Information technology support staff.
 - ✓ Currently the department has 34 staff with only one vacancy, which is a newly created Project Manager position. Since 2020, 13 individuals have been newly hired and 5 more individuals have been promoted to their current position. The IT organization chart appears in Appendix B.
- User training and documentation on Microsoft products including Teams, SharePoint, OneDrive, Outlook, Office 365, Phishing, Fresh Service, Mitel Phones, Adobe, and Zoom.
 - ✓ The team put together publicly available documentation in External Tech Docs under the categories Cybersecurity, ETS, Guidelines, IS Communications, Project Management, Tech Plan, and User Support. Under User Support, an additional 5 subcategories were created with several dozen documents posted to provide user level assistance.
- Communication prior to outages, maintenance, and when new apps are launched.

- ✓ The Technology department has built a culture of transparent processes and communication to provide the best information related to outages possible. Outage requirements and Issues are discussed internally at both various departmental meetings as well as the Change Advisory Board to understand impacts. The refined information is then passed along district-wide to all staff.
- Enhance district and college websites and make them more user friendly and intuitive.
- ✓ The IT department designed a web team consisting of a Principal IT Architect, Sr. IT Analyst, IT Analyst, and the Vice Chancellor and initiated a project to redesign and migrate the district's web site and employee portal from a sharepoint platform to the Modern Campus platform that is standardized across the district.

Forty-four survey respondents answered that they wanted more training:

"I would recommend more training on O365 for faculty and staff."

"Teams and Sharepoint training would be great, as well as how to maximize the use of MS Outlook."

"Yes I would like training on Microsoft Teams and SharePoint."

"More training on phishing."

The Knowbe4 phishing platform that provides user experience and training was implemented in 2021 and has been used successfully with phishing campaigns and training opportunities for all employees each semester.

Survey Summary

For the most requested areas and items shared by survey respondents, the Information Services group has efforts underway to make numerous improvements. We are working to hire additional students to help augment our service desk in taking calls, responding to emails, and helping students, faculty, and staff with technical support requests. There is a significant project underway to update the entire district wireless infrastructure. Once completed, the new wireless networks on both college campuses will provide end users enhanced indoor and outdoor coverage using the latest Wi-Fi technologies. Communication for planned and unplanned maintenance, outages, as well as application and infrastructure upgrades has increased over the last year and will continue. Our cybersecurity training using the KnowBe4 platform was recently launched to assist with security awareness training for our end users. KnowBe4 uses internal phishing campaigns to identify users that need additional focused training, and those efforts will be ongoing. Coordinated end user training will be provided by Microsoft for different areas of Office 365 including collaboration and best practices when using their tools and applications. District Information Systems has training with VMWare scheduled for technical staff in many areas of growth for the department and district including NSX, VDI, Carbon Black, and Vsphere. The district website upgrade to OU Campus is also in progress and once completed will provide a modernized website that is intuitive and easy to use and update.

Improvement of Services Rendered

Improve the Information Systems department follow-through for services rendered.

Results:

- Information Systems department has implemented a CSAT (customer satisfaction) survey which is sent out after support tickets are resolved. This provides an opportunity for the customer to

assess the services rendered as well as an opportunity to re-open cases that need further attention.

- CSAT survey results are reviewed by the Information Systems Director and proactively following up with customers when necessary.

Cybersecurity

A Cybersecurity program has been set up in the IS department including Cybersecurity training and tools for all District employees.

Results:

- District Information Systems designed and rolled out a Cybersecurity program for the district as well as both colleges which included:
 - **(July 2021)** Multi-Factor Authentication (MFA) requirement for all employee groups, with plans to require MFA for students at both colleges this Fall semester.
 - **(August 2021)** Use of Carbon Black, an endpoint protection system which protects against ransomware and malware.
 - **(August 2021)** User account access levels have been optimized to reduce unnecessary administrative-level access to systems, servers, and infrastructure resources.
 - **(September 2021)** MDBR Malicious Domain Blocking and Reporting, which prevents end users from connecting to harmful web domains and internet sites.
 - **(October 2021)** The district has also purchased the Knowbe4 system which includes testing, auditing, and training that has been set up to help staff and faculty increase their knowledge of Cybersecurity. The implementation of this platform will help protect users as well as the district and colleges.
 - **(October 2021)** Keenan Safe Colleges training modules deployed to all employees district wide. Modules included Cybersecurity overview, protection against malware, password security basics, browser security basics, email messaging and safety.

Information Systems projects

District information systems have numerous active and planned projects slated for 2021–2022-time frame. These projects include infrastructure upgrades for the firewall, wired and wireless network, end user Cybersecurity training, Security Incident Event Management, Veeam backup and disaster recovery, and enhanced system monitoring. Here is a schedule of the current and future projects:

2021	2022
<p>Districtwide Infrastructure Change</p> <ul style="list-style-type: none"> • Checkpoint Firewall Optimization • Checkpoint VPN WAN Replacement • Room Alert Temperature Monitoring 	<p>Districtwide Network Refresh</p> <ul style="list-style-type: none"> • Wireless expansion and refresh • Proposed Network Design • Network Switch Replacement RFP
<p>District Firewall Project</p> <ul style="list-style-type: none"> • Firewall Rule Change Management • Firewall Replacement Project 	<p>Backup and Disaster Recovery</p> <ul style="list-style-type: none"> • Veeam Upgrade Project • Veeam site to site replication
<p>Districtwide Cybersecurity</p> <ul style="list-style-type: none"> • Training – Keenan/KnowBe4 • Security Incident Event Management • System Monitoring 	<p>District Infrastructure</p> <ul style="list-style-type: none"> • WVC Generator Upgrade • Bunker Service Relocation • Data Warehouse

Technology goals and strategies

These technology goals and strategies are based upon an institutional program review, accreditation standards, an assessment of internal needs, emerging technologies, and a review of external trends in higher education. The following technology goals are umbrella statements that provide a framework for change.

1. Client Replacement Process: *Create and manage client replacement process.*

Create and manage client replacement process to provide staff and faculty with upgraded technology resources based on emerging technology needs. District Information Systems will assess current inventory to identify and replace devices older than five years and will provide one computer to each full-time staff and faculty member. This process involves arranging a schedule to refresh technology for staff and faculty to support and educate the student population and meet computing requirements. District Information Systems will plan to refresh approximately the same number of staff and faculty computers each year on an ongoing basis.
2. Applications Development: *Develop apps to assist students with educational objectives.*

Develop applications to assist students with educational objectives, Ellucian Degreeworks is used to enhance learning outcomes of students through the development of their individual learning objectives. District Information Systems applications development team will evaluate, develop, research, plan, and test applications, features, and websites for both the district and the colleges. Student education focused web pages, Banner modules and resources are released throughout the year according to the software development life cycle schedules set by the applications team.
3. Server Infrastructure: *Optimize infrastructure for educational resources.*

Manage and support server infrastructure used for education resources, including lifecycle management, providing implementation, maintenance, patching, and eventual retirement of instructional server resources districtwide. The district server group systematically plans, acquires, maintains, and upgrades or replaces technology infrastructure equipment to meet institutional and administrative needs. Ongoing management of the District Information Systems server infrastructure includes phasing out obsolete hardware and software used for managing servers and other infrastructure specific equipment.

Technology consolidation

Information Systems is a central technology services group that partners with the colleges and other district departments to support the technology and infrastructure needs related to teaching, learning, administration, and business processes. Information Systems is most successful when staff and leadership can work directly with partners to understand issues, help define problems that need to be solved and work jointly to implement solutions. Historically, the Information Systems department was seen as a service provider in a consultation role working on a pre-defined scope of work. More recently, a new emphasis has been focused on where the technology department operates more as an active participant who is engaged in delivering a solutions-oriented strategy or service. This includes developing a role based on partnership, transparency, and outstanding customer service. Over the last ten years the perception is that there has been differential funding between the colleges and the goal now is to standardize funding with an emphasis on equity.

This technology plan has successfully identified where the Information Systems department can support the strategic and tactical goals of the colleges and district. The Information Systems department will continue working closely with the colleges and the district to further define the processes. which foster a successful collaboration and identify the specific steps that will be taken to support the identified goals of both the colleges and the district. With these thoughts in mind, the technology partnerships were taken to the next level with a consolidation project that is discussed in the next section.

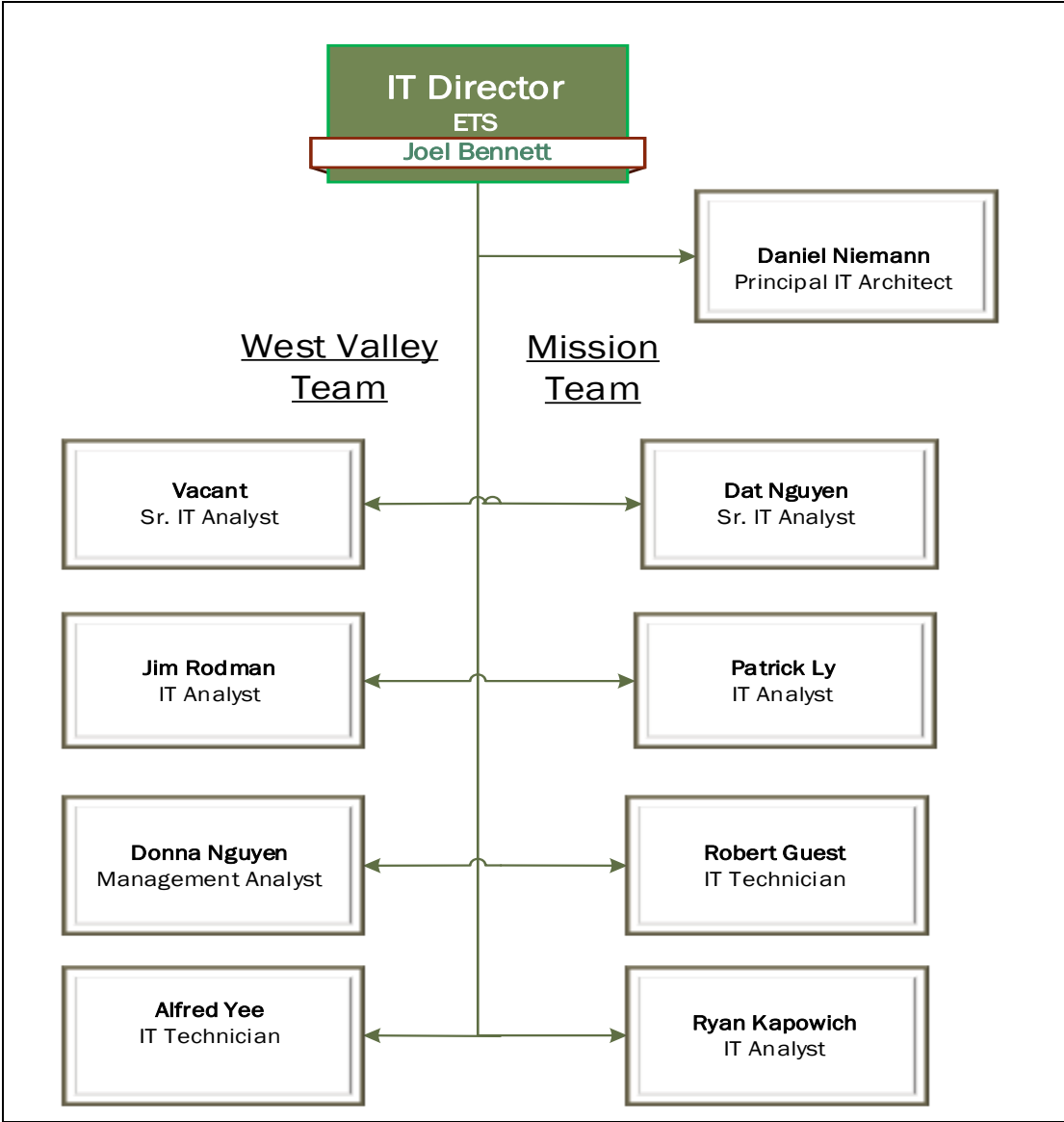
Educational Technology Services

In January 2022 a significant change took place where the three primary areas of technology were consolidated under one Technology Department. Significant organizational change management was needed to bring these areas together to operate more efficiently for all consumers of technology at the district. This included combining the areas of Educational Technology Services (ETS) at West Valley College, ETS at Mission College, and Information Systems at the district. These changes were made to enhance and improve services to all areas including special emphasis and support for Instruction and the student experience using technology to facilitate their educational experience at the district.

The three areas have operated as distinct silos in the past, rarely sharing information, methods, knowledge, expertise, or processes on a regular basis. Each group was used to an autonomous operational strategy and did not generally get assistance for service or support requirements from either of the other two entities. This autonomy proved challenging with significant impacts when making technology decisions affecting staff, faculty, or students at the district. The objective was to put a technology-oriented leadership team in a good position to manage an environment that is constantly changing with new and emerging technology. Additionally, the goal was to address the issue of technology support ambiguity for all users when requesting assistance. Depending on the source area

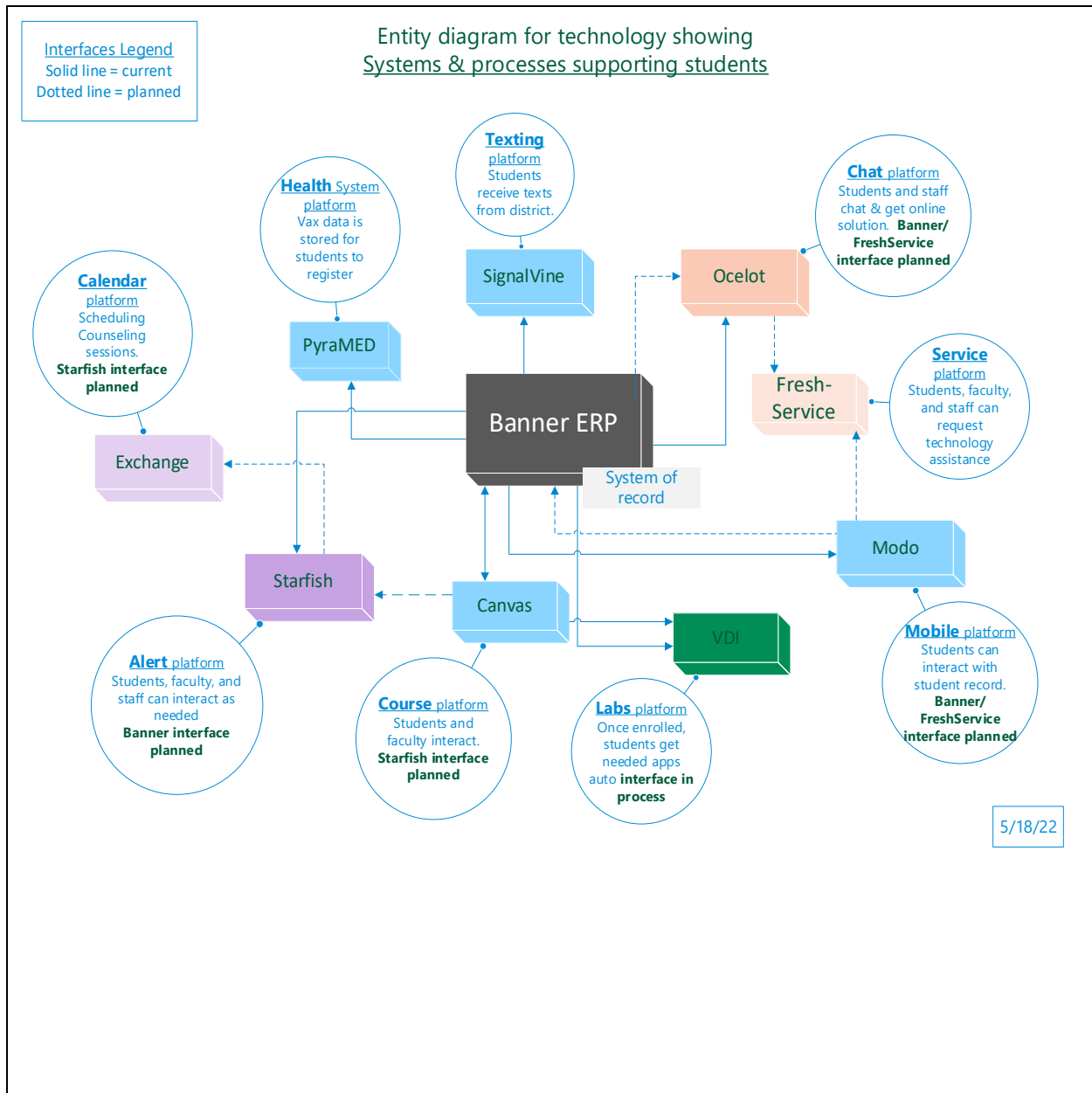
(administrative or instruction) where the technology service is required, people are not sure which service portal to use. This along with other challenges will be addressed over time using teamwork and strong communication strategies. The district has identified a need to create efficiencies and develop student and staff equity by providing efficiencies and a simpler path to all technology resources.

To make this plan successful, the Academic Technology group will follow a similar organizational structure as that of the IS department where team is headed up by an IT Director and a Principal IT Architect and then all staff activities are directed from there. After the change was made, all staff and their assigned duties remained the same in the new organization as they were in the old structure. The new organizational chart appears below:



ETS impact on strategy for Students

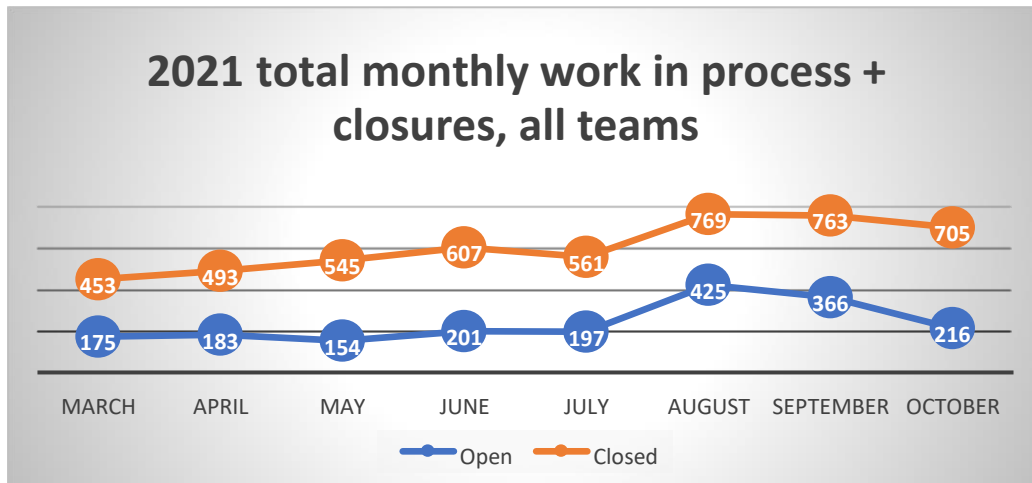
Now that all aspects of these functions now exist in one unified department, strategic opportunities have developed to deliver a cohesive and integrated experience with technology for students to assist with their educational journey. The following system interface chart shows the plan as of 5/10/22:



Appendix A: Fresh Service statistics

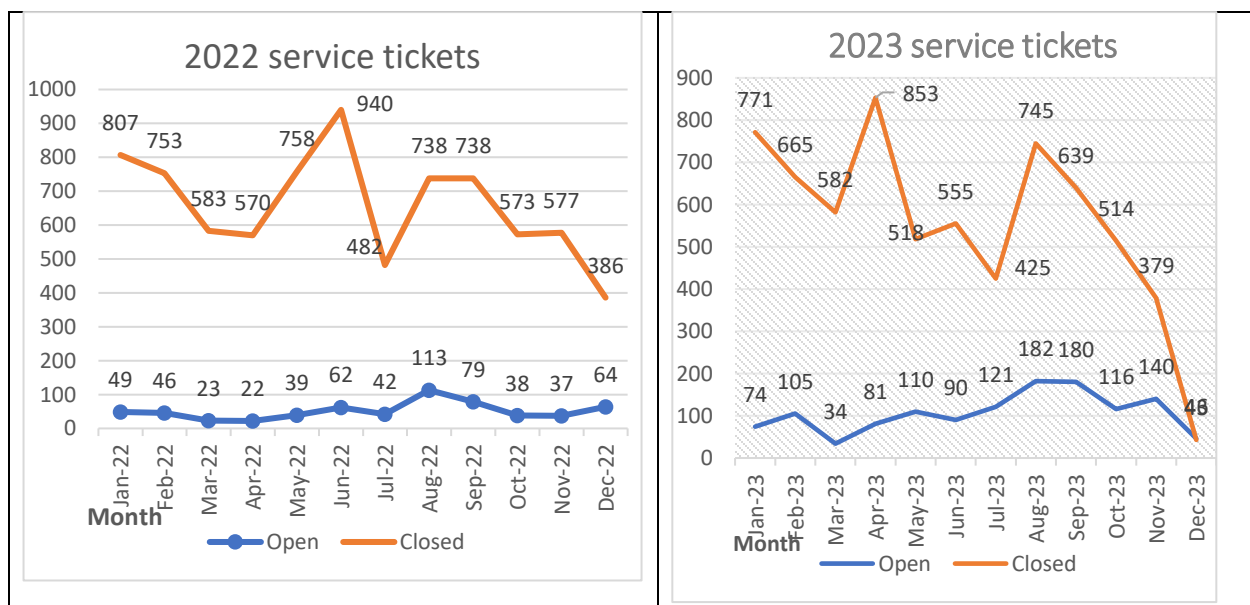
Items in process and closed per month, total for all groups.

Below is a chart of the total monthly tickets opened and closed within the Fresh Service incident ticketing system. Each ticket represents an instance where someone requested assistance from District Information Systems IT support. This chart shows the trends in requests during the year.



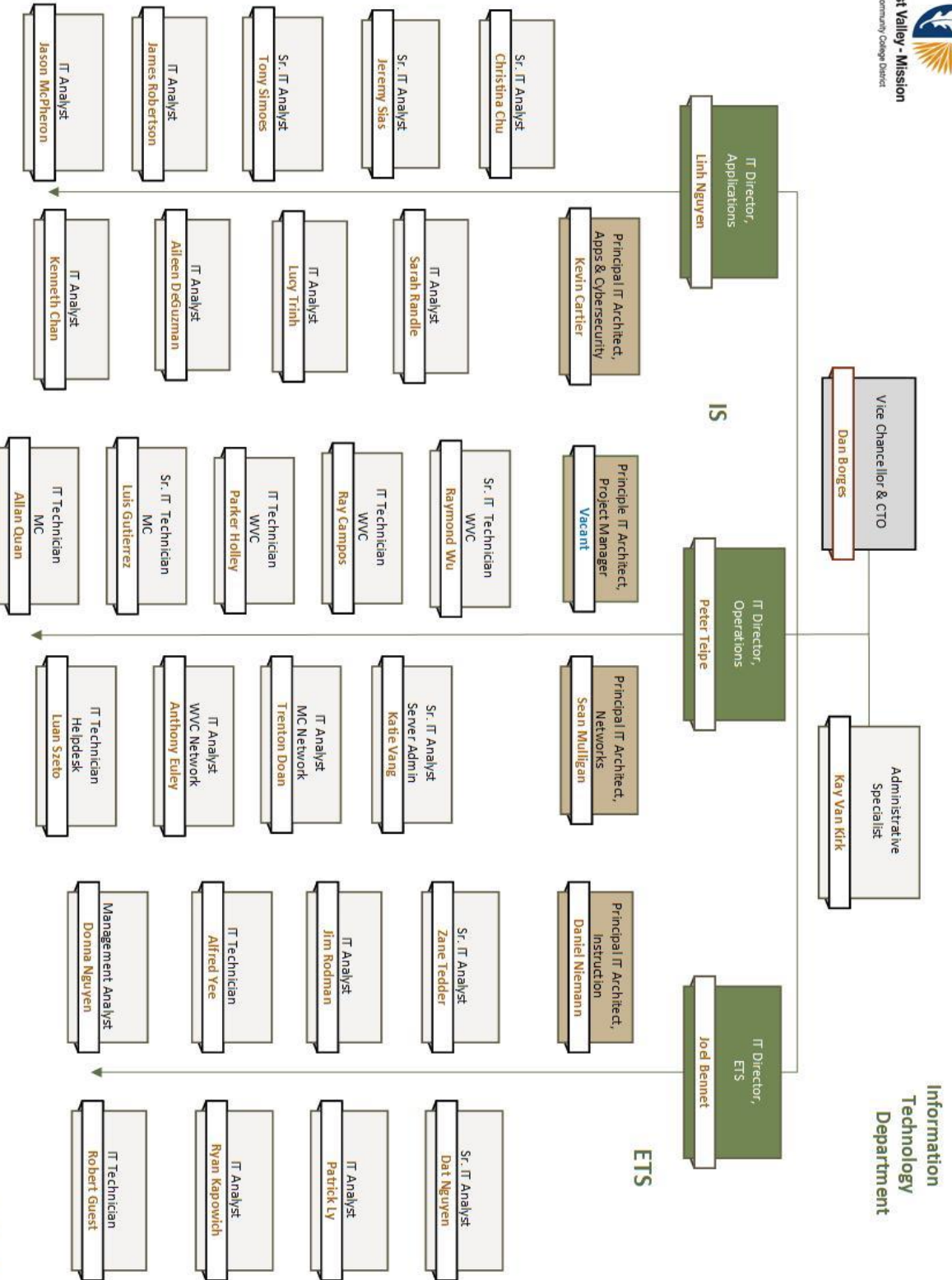
The number of requests received and closed from March to July was consistent, while District Information Systems received an influx of requests for August and September. This was due to the start of the fall term as well as staff and faculty returning to campus.

The two charts below show the volume of tickets that flow through IT. The drop off at the end of 23 resulted from cutting off data acquisition before the end of December. The total number of closed tickets in 2022 was 7905 and the total number of tickets in 2023 was 6689.





Appendix B: IT Department organization chart



as of 12/1/23

Appendix C: NIST Cybersecurity Framework analysis

1. GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood

- Monthly Technology Advisory Coordination (TAC) team meetings provide strategy.
- Knowbe4 user training and phishing simulation processes implemented.
- Contract review with purchasing and IT
- Bi-monthly Change Advisory Board (CAB) meetings provide opportunities to discuss stakeholder objectives.
- Program Review processes at each College are used to collect requirements.

Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

- Weekly executive team meetings (EMT) provide vision and status.
- Regular Cybersecurity meetings are utilized to discuss security issues.
- The State Chancellor's office C1risk assessment system is used to identify and inform institutional cybersecurity risk discussions and strategies.

Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.

- The Software Application Request (SAR) process that has been established in the district's service management system provides tracking and analysis methodology for all Cybersecurity, ADA, and resource allocation considerations.
- Established standard for multifactor authentication (MFA) and use of virtual remote desktop for Vendors and contractors to track and verify proper resource usage.

Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated

- The department leadership is well structured with balanced responsibility and accountability. A Cybersecurity task team has been established and key roles and positions include Vice Chancellor of IT, IT Director of Operations, Principal IT Architect, Applications and Cybersecurity. Additional members include the IT Directors, the Network team, and the Server team.

- The CAB monitors change management in our technology environment and manages cybersecurity risk across the entire department.

Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced.

- The district follows the established guidelines found in the Information Security Program supporting Admin Procedure [AP3721](#)

Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy

- Use of Resolute guard provides objective outside resources to analyze the cybersecurity posture of district processes and system. In addition, IT expertise is used to identify and address risk factors for patching, exploits, and compliance. Once identified, established processes are in place to address and manage cyber risks.

2. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization

Asset Management (ID.AM): Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

- Mixture of AD/SCCM, JAMF, FreshService, and Infoblox cover almost all district assets,
- SCCM and JAMF maintain the list of district software, but users can still load their own untracked software.
- Visio documentation exists for the network flows, and we keep a database for tracking and maintaining the used virtual networks and corresponding firewall security zones

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to the organization, assets, and individuals.

- Weekly tenable scans to identify. Missing next steps of formal process of remediation, currently done ad-hoc
- The district maintains memberships of MS-ISAC and REN-ISAC for information feeds to stay knowledgeable about current risks.
- Although district lacks a formal review process, necessary activity is performed ad-hoc based-on risk scores of vulnerabilities.
- Related discussions take place at one of 3 regular communication opportunities: EMT, CAB, or TAC.
- Although there is currently an Ad-hoc procedure, a formal written process will be documented.

Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions

- Related discussions take place at one of 3 regular communication opportunities: EMT, CAB, or TAC.
- The district has collaborated with the CCCO security contractor as they performed a Penetration Test (Pentest) proving that adequate and (sometimes superior) techniques and strategies have been employed across the district.
- The district has an ongoing relationship with ResoluteGuard, a cybersecurity organization funded through the JPA assisting with processes and procedures.

3. PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk

Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access

- Azure AD, radius for network equipment, and policy to not use default local credentials.
- Employee end-users required to utilize Multifactor authentication for access to resources.
- The Banner ERP system utilized ADAP functionality to provide user provisioning to automate the creation of user accounts in Active Directory (AD) with appropriate rights and access.

Awareness and Training (PR.AT): The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks.

- Keenan and KnowBe4 training libraries are utilized. Also, two large phishing campaigns performed annually with targeted follow-up campaigns as needed.

Data Security (PR.DS): Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- Use of Veeam backup software ensures integrity, availability, and accuracy of District data.
- Processes are followed to remove all storage media from obsolete computers.
- Use of Veeam backup software along with immutable storage ensures integrity, availability, and accuracy of District data.

Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.

- SCCM/JAMF and GPOs are provisioned on workstations/servers.
- Old Operating Systems (OS) and unsupported software packages are removed, or the systems are mitigated with additional network segmentation.

- Logs are sent to the Security Information Event Management (SIEM) system.

Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.

- District building data and telecom closets protected with electronic access controls, radius authentication on network switch, changes to configuration are tracked.
- IT and Facilities leadership has collaborated to create projects to address identified requirements and needs. A lifecycle management program has also been created for rotation of aging infrastructure equipment.
- Offline backups are maintained for critical network infrastructure equipment in the event of hardware failure.

4. DETECT (DE): Find and analyze possible cybersecurity attacks and compromises

Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.

- District managed Palo Alto firewalls are monitored, and events logged for follow up audits.
- Libre and Zabbix are utilized to monitor systems, servers, and infrastructure.
- Firewall traffic and AD logs are forwarded to SIEM for monitoring.
- Zabbix monitoring for expected results from systems to detect manipulations or improperly applied updates that cause a disruption to availability.

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

- Review of SIEM data is used to investigate unusual activity and adjust technical controls as needed.
- Information collected on the SIEM for firewall/network, and host HIDS data.
- Information feeds from MS-ISAC and REN-ISAC and Palo Alto for the firewalls

5. RESPOND (RS): Take action regarding a detected cybersecurity incident

Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed.

- Incident response plan is maintained in the Cybersecurity Teams site for access and centralized updating by the Cybersecurity response team.

Incident Analysis (RS.AN): Investigation is conducted to ensure effective response and support forensics and recovery activities.

- Use of security and HIDS logs from SIEM to identify systems affected.

- Investigation notes are logged in a secondary offline system.
- System images are captured and hashed to authenticate the integrity of the data.
- Once scope of the incident is determined the estimation on remediation and data leakage and impact to the district can be determined

Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.

- Information is shared with risk management team and insurance carrier is involved.

Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects.

- Network segments and system are taken offline to mitigate further spread and to aid in validation/remediation efforts.
- Systems are removed or reimaged from service to reestablish clean systems on the restored environment.

6. RECOVER (RC): Restore assets and operations impacted by a cybersecurity incident

Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.

- Recovery from IR plan using Veeam backups.
- Backups validated via SureBackup. Backup files are stored on immutable storage that is segmented from the operational network.

Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties.

- Use of the portal and fresh service pages are available for sharing incident updates.

Appendix D: Equipment Lifecycle & replacement plan

Description	Systems	Asset Cost	Life Cycle (Years)	Yearly Replacement Cost
Instructional Systems				
Audio Visual Systems Systems	331	\$16,802,800.00	6	\$2,800,466.67
Computer Systems	2318	\$3,490,784.00	5	\$698,156.80
Servers	47	\$1,213,000.00	7	\$173,285.71
	Total Asset Cost	\$21,506,584.00	Total Replacement per year	\$3,671,909.18
2024-25 Instructional Systems Critical Replacement				
Sci and Math Audio Visual Systems Systems	13		12	\$580,000.00
Servers	6		7	\$61,000.00
			2024-25 Total	\$641,000.00
2025-26 Instructional Systems Critical Replacement				
LASS Audio Visual Systems Systems	13		13	\$710,000.00
Servers	6		8	\$61,000.00
			2025-26 Total	\$771,000.00
2026-27 Instructional Systems Critical Replacement				
LASS Audio Visual Systems Systems	13		13	\$710,000.00
Servers	7		7	\$219,000.00
			2026-27 Total	\$929,000.00
Staff Systems				
Computer Systems (desktops)	500	\$750,000.00	5	\$150,000.00
Computer Systems (laptops)	280	\$336,000.00	5	\$67,200.00
Computer Systems (HP Printers)	141	\$126,900.00	5	\$15,000.00
Infrastructure (network switches-core/datacenter) - adv price	13	\$1,430,000.00	8	\$110,000.00
Infrastructure (network switches-access) - advert. price	162	\$8,586,000.00	7	\$1,226,571.43
Infrastructure (Firewalls) - list price	4	\$421,000.00	5	\$84,200.00
Infrastructure (Wireless APs Internal) - list price	550	\$1,375,000.00	7	\$196,428.57
Infrastructure (Wireless APs External) - list price	110	\$319,000.00	6	\$53,166.67
Infrastructure (Servers) - list price	8	\$108,000.00	7	\$15,428.57
Infrastructure (UPS units)	215	\$1,290,000.00	7	\$184,285.71
	Total Asset Cost	\$11,649,900.00	Total	\$1,917,995.24
2024-25 Staff Systems Critical Replacement				
Computer Systems (client computers)	150	\$1,800.00	5	\$270,000.00
Computer Systems (laser printers)	16	\$900.00	5	\$15,000.00
Infrastructure (Servers) (Infoblox appliance only)	2	\$6,000.00		\$12,000.00
Infrastructure (UPS units)	7	\$184,285.71		\$184,285.71
			2024-25 Total	\$481,285.71
2025-26 Staff Systems Critical Replacement				
Computer Systems (client computers)	150	\$1,800.00	5	\$270,000.00
Computer Systems (laser printers)	16	\$900.00	5	\$15,000.00
Infrastructure (UPS units)	7	\$184,285.71		\$184,285.71
			2025-26 Total	\$469,285.71
2026-27 Staff Systems Critical Replacement				
Computer Systems (client computers)	150	\$1,800.00	5	\$270,000.00
Computer Systems (laser printers)	16	\$900.00	5	\$15,000.00
Infrastructure (UPS units)	7	\$184,285.71		\$184,285.71
			2026-27 Total	\$469,285.71

Appendix E: IT Fixed Cost allocation 2023 -24

Ref#	Vendor	Service	Type	Cost
H.1	Adaptigent	NetCOBOL Linux x64 - Maint/support	Hdw	\$1,901.00
S.1	AdArt	Scala Content Manager	SW	\$8,250.00
S.2	AdAstra	Scheduling Software (facilities rental) - MC/WV	SW	\$42,421.00
S.3	Apple	Jamf Protect EDU & Jamf Pro iOS	SW	\$30,354.00
S.4	Arveva	Exceed Further:	SW	\$4,765.00
H.2	AT&T	Telephone Expenses	Hdw	\$211,000.00
H.3	Avtech	Room Alert Professional Monitoring	Hdw	\$699.95
S.5	Award Spring	Online scholarship management platform.	SW	\$0.00
S.6	BrowserStack	BrowserStack	SW	\$2,507.00
S.7	CCCApply	Online Admissions Applications - MC/WV	SW	\$11,800.00
S.8	CDWG ProofPoint	Email security software	SW	\$60,135.00
H.4	Citrix	Citrix Load Balancers x2	Hdw	\$0.00
S.9	Cloudinary	Cloudinary	SW	\$2,688.00
S.10	ComputerLand	Microsoft Campus Agreement	SW	\$92,195.00
S.11	ComputerLand	Microsoft Campus Agreement	SW	\$96,961.00
S.12	Computerland	VDI Students for Adobe suite	SW	\$35,991.00
S.13	ComputerLand	Adobe Creative Cloud	SW	\$58,327.00
S.14	ComputerLand	Adobe Student Named Licenses x50 (MC) and x108 (WV)	SW	\$12,636.84
S.15	ComputerLand	Filemaker Pro	SW	\$595.00
S.16	ComputerLand	Patch my PC cybersecurity	SW	\$0.00
H.5	Dasher	HP Blades-for Server Support Synergy	Hdw	\$0.00
H.6	Dasher	HP 8212 network switch Aruba	Hdw	\$12,096.00
H.7	Dasher	HP Aruba 54xx and 29xx	Hdw	\$37,167.82
S.18	Dasher	Veeam Back-up Recovery & Data Management	SW	\$0.00
H.8	Dell/Apple	Equipment replacement/repair	Hdw	\$100,000.00
S.19	DocuSign	DocuSign - Annual Maint.	SW	\$107,312.00
S.21	EAB Starfish	Student online solution/services - WVC	SW	\$68,252.00
S.22	Ellucian	SmartBen to Banner Custom Batch Interface Maintenance	SW	\$37,363.00
S.23	Ellucian	ADAP Adapter Mod Maintenance	SW	\$7,178.00
S.24	Ellucian	Banner Hosting Services (AHS)	SW	\$661,896.00
S.25	Ellucian	Oracle (HOSAL) App Server & Relational Database Syst	SW	\$126,215.00
S.26	Ellucian	Banner Core Modules	SW	\$340,108.00
S.27	Ellucian	Campus Logic - Student F	SW	\$82,600.00
S.28	eLumen	Curriculum & Assessment Mngt for SLO - MC/WV	SW	\$75,999.00
S.29	Evisions	FormFusion for POs	SW	\$7,822.00
S.31	FormStack	Software service for forms	SW	\$23,542.00

Ref#	Vendor	Service	Type	Cost
S.32	Fresh works	Fresh Service Helpdesk	SW	\$92,447.04
S.33	GoDaddy	SSL Certificate MC/WV	SW	\$700.00
S.34	Indiana University	Institutional Security Membership REN-ISAC, cybersecurity	SW	\$1,375.00
S.35	InterVision	InfoBlox	SW	\$29,390.00
S.37	Intrado Life	Intrado, cybersecurity	SW	\$25,223.00
S.38	IP Quality Score	Student fraud system	SW	\$35,982.00
S.39	ITC Group	GoPrint Software Maintenance	SW	\$14,314.70
H.9	KIS	ExaGrid	Hdw	\$2,685.00
S.40	KIS	Veeam Server Management	SW	\$53,963.70
S.41	KIS	VDI client security/ Carbon Black	SW	\$26,509.00
S.42	KIS	VMWare - ULA software	SW	\$449,000.00
S.43	KIS	Ekahau Wireless Survey	SW	\$3,580.00
S.44	KnowBe4	Cyber Security Training	SW	\$21,060.00
S.45	Modern Campus	Omni Update Web CMS	SW	\$93,097.00
S.46	ModoLabs	Mobile app for Student, Fac, Staff	SW	\$89,653.00
S.46	ModoLabs	Mobile app for Student, Fac, Staff	SW	\$36,765.78
S.47	N2N	N2N App intragator	SW	\$49,600.00
S.48	NameCoach	LTITool	SW	\$0.00
S.49	NetNet Hosting	Hosting - monthly and maint.	SW	\$17,640.00
S.50	Ocelot	District Chatbot	SW	\$60,000.00
H.10	Pacific West	Sonitrol alarm system	Hdw	\$14,401.00
S.52	Packet Fusion	Mitel Support	SW	\$67,658.16
S.53	Panopto	Video Platform for WVC	SW	\$98,000.00
S.54	Recast	Security Compliance, cybersecurity	SW	\$17,788.00
S.55	Sanako	Sanako (MC/WVC)	SW	\$21,450.00
S.56	Scantrol	Scanners and software - MC/WVC	SW	\$14,160.00
S.57	SignalVine	Text Messaging Platform - MC & WVC	SW	\$45,120.00
S.58	Smartsheet Inc.	Smartsheet Licenses	SW	\$11,952.05
H.11	SYSTAT	UPS Unit server	Hdw	\$53,029.00
H.12	T-Mobile	Radio/Cell Phone Service	Hdw	\$18,920.00
H.13	Trivad	Cisco SMARTnet-service contract	Hdw	\$400.00
S.59	Twilio	Student text messaging	SW	\$1,329.00
S.60	Zoom	Zoom Licenses	SW	\$43,196.00
S.61	Ellucian	Campus Logic - Student F	SW	\$82,600.00
S.62a	CCLC	Turnitin - Plagiarism ched	SW	\$18,088.16
S.62b	CCLC	Turnitin - Plagiarism ched	SW	\$15,223.00

Appendix F: External Wireless heat map for West Valley College



Appendix G: External Wireless heat map for Mission College



Appendix H: 2022-2023 Accomplishments

The following information provides some of the accomplishments that have been achieved over the previous two years.

2022

- Incorporated Educational Technology Services (ETS) staff into newly created group and hired IT Director and Principal IT Architect focusing on academic technology.
- Published 2022-2025 Tech Plan after meetings with shared governance groups:
- Implement custom Non-Credit application process.
- Create new Class Search to meet student needs.
- Implement Ocelot, Degree Work 5.0.7.2, and Global FSA.
- Build Starfish & Banner integration for MIS reporting.
- Enhance the ADAP process and Email Distribution Listing.
- Enhance the Student and Employee onboarding process.
- Roll out SSB9 General Profile & Student Profile.
- Replaced aged Checkpoint Firewalls with Palo Alto network infrastructure improving security.
- Deployed Carbon Black and Jamf to all admin and academic workstations improving security.
- Setup Wireless network Request for Proposal and selected vendor for implementation.
- Implemented new Student System strategy with Banner interfaces to 9 separate platforms.
- Facilitated and receive Board approval for BP 3721 Information Security
- The Data Center redesign project has been scoped and funding sources are being identified.

2023

- WVC Visual Arts AV deployment in 6 classrooms
- MC Business & Tech AV deployment in 19 instructional spaces
- Online course catalog was deployed for students to easily access the data during a web session.
- System Center: Pxe boot + Computer patching & inventory management.
- Developed cyber security user awareness campaigns and training for all faculty and staff.
- Wifi infrastructure deployment for all internal spaces
- Implemented Starfish for Instruction and Student Services to collaborate on student success.
- Implemented non-credit application process.
- Setup Class Search process to present Banner data more intuitively in Banner.
- Setup Ocelot Robo and Live chat AI application to assist students with answers to frequently asked questions.
- Implemented Fraud Tracking system for A&R, Financial Aid, and Office of Instruction to review data points and put hold on fraudulent records.
- Implemented ARC Facilities software suite for Facilities management.
- Police communication upgrades which included new interface equipment in each vehicle and a new E911 system to help first responders locate 911 calls made from the district's network.

Appendix I: 2024- 2025 Goals and objectives

In the coming months and years, the following list includes the IT department key priorities for 2024-2025. The objectives are separated by each of the 3 primary groups.

ETS

AV Design for WVC Learning commons which will include 48 new instructional spaces.
Virtual systems design and implementation for Instruction computers at Mission College.
Authentication badging system for students and faculty using digital student IDs with Multi Factor Authentication (MFA).
Ocelot to Banner integration to support the Modo unified student portal

Operations

Network infrastructure & IDF management / upgrades using ARC Facilities
Deliver Data Center infrastructure upgrade to improve power and HVAC at the WVC DC.
Setup and configure Security Information Event Management (SIEM) platform to collect cyber security metadata to analyze and remediate.
Build out service management system to include additional district departments.
Continue to enhance Cyber security protection.

Applications

Implement Campus Logic to assist students with easy submittal of Financial Aid documents.
District Website platform upgrade from Sharepoint to Omni Update Modern Campus improving functionality and interface.
Electronic document management for HR paperwork.
Banner SSB 9 functional upgrade.
Build integration required for MIS reporting between the Starfish and Banner data systems.