Fort Bend Independent School District

2022 Technology Master Plan

As of May 1, 2022

INTRODUCTION AND BACKGROUND

Fort Bend ISD (FBISD) has experienced a tremendous increase in the adoption and use of technology across its environment for the past eight years, accented by the needs for remote learning during the pandemic.

Fort Bend ISD students and employees were fortunate to have the Fort Bend County communities' support in approving the 2014 Bond where the fund was used to renovate FBISD's digital infrastructure, providing ubiquitous bring-your-own-device (BYOD) wireless access throughout the district and a high-speed, resilient network that have supported the increasing digital demands. Bond 2014 provided for the upgrade of district network backbone from 1Gbps to 10Gbps for Internet access capability and firewalls that protect FBISD digital ecosystems. With funding from Bond 2014, FBISD data center infrastructure is now a Tier II data center, capable of providing higher availability and redundancy for mission critical applications and network stability. The data center is equipped with a physical and virtual server environment that provides the computation horsepower to run critical applications such as PeopleSoft, storage, SQL databases, web services, etc. Finally, Bond 2014 provided an extensive camera network and storage that has enhanced security throughout the district.

FBISD communities again overwhelmingly provided its support to enhance FBISD technology environment in approving the 2018 Bond. In addition to a learning management system, Schoology, the Bond funds were used to equip every classroom with standard Classroom Toolkit where a ratio of one laptop is provided for every two students. Bond 2018 equipped each campus with Lending Library carts for students to check out a device just as they would a library book. The supply of classroom/Lending Library laptops were instrumental in facilitating online learning during the pandemic. The laptops allowed the district to provide a laptop to students who needed a device to continue their education online. Bond 2018 also provided opportunities for the district to equip each classroom with a Smart interactive board, allowing FBISD teachers with enhanced instruction delivery tool.

Technology continues to fill every aspect of FBISD academic and operational environments. The technology ecosystem can simplify collaboration and communication, empower daily lives, add value to the student experience, and inspire creativity in teaching and learning. For FBISD to realize its mission and vision to our students, these new and increasingly complex technology infrastructures need to be current and reliable for optimal use, in addition to bring enhanced educational experience to our students.

As stated in FBISD's 2014 Technology Infrastructure Master Plan, "technologies, while always the "tools" and not the "ends in themselves," can and will play key roles in the learning environment." The 2022 Technology Master Plan is designed to ensure that information technology priorities and initiatives are targeted to support FBISD's mission and vision. Prioritization and coordination of technology planning and implementation will ensure that

FBISD students, teachers, and staff have the combination of skills, knowledge, and technology to succeed in a technology-rich future. A comprehensive and active master plan that focuses on human and financial resources will create the necessary technology infrastructure that provides a technological environment to help "to inspire and equip all students to pursue futures beyond what they can imagine."

The 2022 Technology Master Plan is developed with the intent to enhance and expand Fort Bend ISD technology infrastructure and systems to support education and its digital needs, which include more than simply providing computers and software. As with the previous Technology Infrastructure Master Plans and 2018 Education Master Plan, best practices and industry standards will continue to lay the foundation.

This plan is a working document that will be revised and updated each year as technology changes or digital demands require the district to change its approach. It is flexible with specificity to serve as a guide in decision-making and budgeting. The recommendations contained in this master plan are intended to provide direction for the Board of Trustees, the Superintendent and the Executive Team, principals, teachers, support staff, parents, and students in planning for technology infrastructure projects for the near future.

I. Large Venue Video Refresh

Bond 2018 provided the funds needed to address the need to replace old and outdated audio/video at campuses in the auditoriums, cafetorium and libraries; however, large venues at five high school auditoriums still have outdated video equipment, AHS, CHS, MHS, RPHS, and THS. Refreshing the equipment will provide FBISD Fine Art students with modern video equipment to enhance their wonderful performances.

II. Classroom Device Refresh

Bond 2014 and Bond 2018 have provided FBISD with the computing devices needed for daily use. Each device serves a critical role in instruction delivery, business, life-safety, security, or support in FBISD. Maintaining the health, functionality, compatibility, and reliability of these systems is critical to the on-going success of the district. The Texas Department of Information Resources in their 2021 update to "PC Life Cycles – Guidelines for Establishing Life Cycles for Personal Computers" provides:

> *Personal computers are the primary productivity tool used by most state agency personnel. PCs constitute one of an agency's most volatile, prolific, and mandatory expenditures. While some agencies may have only a few employees, other agencies may employ thousands. Similarly, some agencies utilize more PCs than others, depending on how essential these tools are for delivering agency services. [To] address these issues and concerns, Texas has identified what a reasonable PC life cycle is. A PC life cycle describes the usefulness of a desktop or laptop computer to the agency, from its initial acquisition through its ultimate disposal. A life cycle is determined based on end-user needs, technology changes, and the cost to support technology. The current industry standard for a desktop computer is 4 to 5 years, while that of a laptop computer is 3 to 4 years.*
>
> *The life cycle for laptops should remain within the range of 3 to 4 years. Usage dynamics such as the mobility of laptops reduce their durability. Industry research indicates that expected failure rates of 20% could be expected for laptops due to mobility damage alone.*

While the State of Texas recommends the adoption of a lifecycle of 3-5 years, FBISD has adopted a 5 to 6-year device lifecycle, five years for laptops and six years for desktops. This strategy decreases the district's annual cost for devices by keeping all devices in service for an additional year beyond the State's recommended lifecycle. While devices in their 5th year are certainly slower than newer devices, FBISD has found that through regular preventative maintenance, patching, and user training, we are able to extend devices for an additional 1-2 years beyond the recommended lifecycle with minimal impact on user experience. Extending the device's lifecycle even further would not be recommended. FBISD data show that laptop and iPad battery failures increase significantly in year four and spare parts become extremely difficult to source for six years old laptops/iPads or seven years old desktops.

Most FBISD users (students and employees) use a desktop, laptop, or iPad daily. Thus, having a reliable device that can run the required applications is no longer optional in 2022 and beyond. In fact, in school year 2022-2023, the State of Texas requires that all STARR tests be administered online using district-provided computers. These computers must be able to hold a battery charge for the duration of the test, be compatible with the testing systems, and be responsive enough to not impede a student's ability to demonstrate their required knowledge of the material.

Of the requested funding in the 2022 Bond to maintain the FBISD computer fleet through 2026, 91% will be used on devices for students and 9% for devices for staff.

A. **Classroom Toolkit Refresh:** The current classroom technology model in FBISD is known as the "Classroom Toolkit." This model consists of several technology standards for the classroom. The main feature is the student device cart (sometimes referred to as a COW – Computers on Wheels). Every in-use classroom is equipped with a cart of student devices in an approximately 2:1 ratio (secondary classrooms have 15 devices while elementary classrooms have 12 devices). PreK through 1st grade have iPads while 2nd through 12th grade use Windows-based laptops. This project will replace existing laptops and iPads that are five years or older and will account for estimated increase student enrollment based on the current Population and Survey Analysts (PASA) student enrollment projection. This number also includes an annual loss/damage-beyond-repair rate of 5%. Across the area, most districts see a loss rate of between 8%-10%; however, FBISD has been able to maintain a lower-than-average loss rate due to student/staff training, in-house repairs, and strong classroom management protocols by our teachers.

B. **CTE (Career and Technical Education) Devices Refresh:** Many of the courses offered within FBISD's CTE programs require hardware with greater computing power than the district's regular classroom toolkit devices. Courses such as Architecture, Audio/Video Production, Engineering Design, etc., require faster CPU, more memory, and higher screen resolution. These specialty desktops and laptops come at a higher cost and are often deployed in a one-to-one (1:1) ratio to meet the specific needs identified by the CTE Department.

C. **Staff Devices Refresh:** Over 78% of FBISD employees need a dedicated computer to perform their job responsibilities and over 7,000 of those are laptops. Bond 2018 allowed the District to refresh all teacher laptops in addition to some staff devices; however, over 1,700 staff laptops will reach five years of life and 3,200 desktops will reach six years in the next four years. Additionally, while staff loss/damage is lower than student devices, loss/damage replacement must be accounted for. Based on past year's data, FBISD has a loss/damage-beyond-repair rate of 3% which beats the national average of 5.3%.

D. **Child Nutrition Point-of-sale Devices Replacement:** There are 225 cafeteria registers that will age out over the next four years and will need to be replaced to ensure compatibility with vendor's software and to facilitate the serving times for our students.

To refresh the district's fleet of computers and laptops or provide a 1:1 classroom environment will require both funding from a Bond for the equipment and from the General Fund for desktop analysts to support. If funding is not available, the current Classroom Toolkit environment with 2:1 student to laptop ratio may need to continue.

III. Data Center Infrastructure

Prior to 2014, the District had a single data center located in the Administration Building. The data center is made up of physical facilities, electrical power, uninterrupted power supplies (UPS), generator, air conditioning, and security to support the district's comprehensive information and telecommunication systems. The data center serves as the core of the district's data and voice network, servers, data storage, applications, and Internet for all student and business data and voice services. Previous Bond allowed the District to renovate and rebuild the data center infrastructure that is now a Tier II data center, capable of providing higher availability and redundancy for mission critical applications and network stability. As with other infrastructure equipment, the time has come to refresh the components of the data center, allowing the data center to continue to provide higher availability and redundancy for FBISD mission critical applications and network stability.

A. **Data Center HVAC, UPS Refresh**: Current data center UPS batteries were installed in 2016. The anticipated lifespan of UPS batteries is 4-5 years. While the UPS and associated electronic/electrical components are within the prescribed lifespan of 5-10 years; the UPS batteries need to be replaced to ensure predictable and reliable operation until at which time the UPS and associated hardware can be replaced.

B. **Colocation DC at Austin High School**: Fort Bend ISD currently has two data centers. The primary data center at the Administration Building provides essential services supporting many aspects of district business and educational technologies, including servers, storage solutions, secondary/failover Internet connection, wireless controllers, data center infrastructure services, etc. These systems collectively make up the backbone infrastructure of the district data center and support key district services and applications to include Peoplesoft, Video Insight (security cameras system), shared data storage and many other systems.

A secondary data center supports the primary data center as part of the district's disaster recovery and business continuity plan. The secondary data center's role is to support critical data center operations in the event the primary data center is offline. Currently, the secondary data center is housed in a leased 3rd party data center outside FBISD area. There is an annual cost to maintain and support this service and is projected to increase over the next two to three years. Building a secondary data center in an existing space at Austin High School (AHS), one of FBISD core network sites, will allow a reduction of long-term operating costs and allows a faster response time to recover from a failure in the primary data center.

C. **Data Center Core Network and ACI (Application Centric Infrastructure) Refresh:** The data center core network is the backbone of the data center that provides transport services throughout various systems in the data center such as compute, storage, etc. The current data center core network was installed in 2016 while the Cisco Application Centric Infrastructure (ACI) was installed in 2017. Data center systems rely on a robust and reliable network to communicate and perform at peak levels. The recommended refresh cycle for data center servers and the associated network is five to seven years to keep pace with advancement with energy efficiencies, microprocessor advancements, compression of storage technology which facilities faster, cheaper, and consolidated equipment footprint. Current equipment used within FBISD data centers has reached seven-year age and exceeds the manufacturer's recommended refresh lifecycle. Refreshing this data center infrastructure is vital to supporting the ongoing demand for data center resources but also to ensure the district is not at risk of vulnerabilities and threats posed by outdated and unsupported software and hardware.

The data center network infrastructure is made up of various layers of network switches that include core network layer as well as data center network access layers. The manufacturer has announced end-of-life for most of the data center network; however, the support for this hardware will continue until March 2024. The industry best practice is to refresh equipment prior to the end-of-support of existing equipment so that newly replaced equipment has a period to stabilize the environment.

D. **District Server/Storage Refresh:** FBISD's primary data center and the associated server and storage infrastructure support many FBISD's technology needs. This infrastructure has provided a solid backbone for key applications such as Peoplesoft, security camera system, file storage among many other applications. The current storage capacity of the primary data center is 425 TB of which 85% is currently allocated and used to support various districts' storage needs. Additionally, the district currently has 14 physical servers that support 380 virtual servers, hosting numerous applications. The funding will expand the capacity to and will ensure the district is able to purchase additional storage as the demand for storage and servers increases over the next 3-5 years.

IV. Network Services

The data network consists of the wide-area network, the local-area network, and the wireless network. These networks provide the core transport mechanisms for the data and voice traffic from one campus to another campus, to the data center, and/or to the Internet. Bond 2014 provided the funding for the district to rebuild the network that can support 10 Gigabits per second (Gbps), fiber optic network paths from each campus to the data center. In addition, a ubiquitous wireless infrastructure allows the district to use different wireless solutions in the classroom and enable our students the ability to bring their own devices. The network has and continues to serve the district and our students well over the past seven years.

A. **LAN/WAN/Wireless Network Refresh Cycle For HS, MS, ES & Support Sites:** The Local Area Network/Wide Area Network (LAN/WAN) and Wireless networks collectively form the backbone of FBISD's information superhighway. FBISD's network was previously redesigned and refreshed starting in 2015 as part of the 2014 Bond. The redesign and refresh provided for a robust, resilient, and reliable network that has provided essential networking services to all areas of Fort Bend ISD. The 2020 COVID pandemic, the resulting transition to online instruction, and the continued growing number of personal (BYOD) and district devices have confirmed the need of network expansion to meet the demands.

   The industry recommended lifecycle refresh for network technologies is 5 – 7 years. FBISD's network will reach the seven-year mark in 2022. FBISD LAN (Local Area Network) is configured with two primary network layers, distribution layer and access layer. Distribution layer switches throughout the district serve as an aggregation point for the campus, these switches have exceeded the recommended manufacture lifecycle. The manufacturer announced the end-of-life for these switches in October of 2019, followed by end-of-software maintenance as of Oct. 2021. Finally, the end-of-vulnerability/security support will end October of 2023. Similarly, all access layer switches throughout the district have reached end-of-life as of October 2019, end-of-software maintenance as of October 2021, and end-of-vulnerability/security support as of October 2023. Network lifecycle refresh is essential to maintain availability, security, and stability of the FBISD computing environment.

   FBISD wireless infrastructure has also served FBISD instructional and business environments well. The infrastructure has become very outdated. The current wireless controllers are reaching end-of-life and end-of-software maintenance as the LAN switches are. The current wireless access points were installed between 2015-2018 and most access points are 802.11ac (Wi-Fi 5) technology. To fully prepare for current and future wireless technologies, FBISD wireless infrastructure will need to undergo a refresh to 802.11ax (Wi-Fi 6) infrastructure that will provide a more reliable/compatible, higher wireless bandwidth, and more secured wireless environment. Wi-Fi 6 was introduced in 2019 and will replace 802.11ac as the de facto wireless standard, capable of providing a maximum 10Gbps wireless connection to the end device when the wireless standard reaches its maturity.

B. **Secondary Firewall:** With the emergence of constant cybersecurity threats to the K-12 environment, firewalls provide the necessary defensive components for FBISD computing environment. FBISD network has two firewalls in the data center that are capable of defending FBISD network against any cyber-attack from the Internet and providing Internet filtering as required by the Child Internet Protection Act (CIPA). A second set of firewalls are needed at the secondary data center to provide redundancy and failover support for the primary firewalls. Secondary firewalls play a critical role in support of disaster recovery and business continuity for FBISD. These firewalls are designed to function as a backup security system in the event the primary firewalls at the main data center are off-lined. The current firewalls at the secondary data center were installed in 2018. The industry standard lifecycle for perimeter security hardware such as firewalls is 5-7 years. The manufacturer has announced the current secondary firewalls in use are end-of-support as of January 2024 and will need to be replaced during the next two to three years.

C. **UPS Refresh**: An uninterruptible power supply (UPS) is an electrical device that provides emergency power when the main power source fails. UPS systems are part of the network infrastructure technology at all locations throughout the district. The district has over 350 IT (Information Technology) network closets that provide network connectivity to campuses and buildings. UPS systems are essential to minimizing network outages and disruption of classroom instruction and daily district operations. The current UPS systems were installed as part of network infrastructure refresh starting in 2015. Under normal operating conditions, the estimated lifecycle of a UPS system is eight to ten years (excluding batteries); however, several factors impact the longevity and life of a UPS system such as ambient temperature, number of discharge cycles, voltage variations, number of brown-out and power surges. The UPS systems will need to be refreshed in the upcoming two to three years.

UPS' batteries have limited life, usually showing a slow degradation of capacity until they reach 80% of their initial rating, followed by a comparatively rapid failure. As with the UPS system, there are four primary factors that affect batteries' life: ambient temperature, battery chemistry, cycling and service. The Institute of Electrical and Electronics Engineers (IEEE) association defines "end-of-useful life" for a UPS battery as being the point when it can no longer supply 80% of its rated capacity in ampere-hours. In 2021, the district started a UPS Battery Refresh Project with the scope of replacing UPS batteries in all network infrastructure closets. This effort will extend the life of the UPS units for another 2-3 years, at which point the UPS must be replaced.

V. Voice Services

Telephones throughout all areas of the district continues to provide an essential function to support daily district operations. The 2018 bond funded the replacement of 6,750 phones and accessories throughout the district which covered schools, offices, and other support areas.

A. **Telephone Replacement**: In 2022 Bond, the district is seeking to replace the remaining list of outdated and unsupported phones. The phones on the list to refresh includes models for which the manufacturer announced end-of-life as of December 2017. Additionally, these same models no longer have software maintenance support as of June 2019 and the last day of support is June 2023.

   Refreshing these outdated phones will ensure district staff and teachers continue to have reliable phones to support day-to-day duties and will allow the district to serve the students and the community.

B. **SIP (Session Initiation Protocol) Migration**: The SIP is a signaling protocol that enables the Voice Over Internet Protocol (VoIP) by defining the messages sent between endpoints and managing the actual elements of a call. SIP supports FBISD with voice call capabilities. Currently, the district is using a legacy voice technology for voice trunk connection, Primary Rate Interface (PRI) that is a 1980s voice technology. PRI is a telecommunication interface standard primarily used in Integrated Services Digital Networks (ISDN) and will need to be replaced with the modern SIP voice trunks. SIP is a scalable solution that has the potential to reduce ongoing operations costs. In addition, telephony companies will start to phase out ISDN technology during the upcoming years.

VI. Systems

A. **ERP (Enterprise Resource Planning) Retool or Replacement:** ERP Financials was installed in 2006 and HCM (Human Capital Management) module was implemented in 2007. Throughout the years, the district has upgraded the application, Peoplesoft’s tools and database as required. FBISD has made a significant investment in the current systems that are in place and PeopleSoft support will continue until 2033. Various development projects and customizations have been built by district staff to provide business functionalities that are needed to improve processes, reduce manual work, capture data that otherwise would not have a designated location in PeopleSoft. There are several PeopleSoft modules that could be implemented to facilitate additional manual processes and streamline business operations. Since the ERP was originally implemented over 16 years ago, a collective decision was made to process a request for proposal (RFP) for a new ERP system. This was completed in October 2021. FBISD has also worked directly with Oracle to obtain an estimation of what it would take to implement new modules and correct some of the laborious processes that were created by or since the original implementation. FBISD is still in discussions with Oracle to refine the scope of work for both HCM and Financials with prioritized critical business functions. The estimate for funding will include licenses, consulting services, and backfills for designated project staff during project implementation for the retooling of the existing ERP environment or purchasing/installing a new ERP. The estimated funding will be a part of a future bond or would be funded out of bond contingency.

B. **Data Warehouse**: FBISD has many disparate sources of data, ranging from student data to human capital resource data and more. Many of the data sources are divided into different data sets that feed into different systems. For example, student data, student achievement data, human resources data, financial data, asset tracking, special education, food services, and professional development feed into different reporting systems. Integrating data from one or more disparate sources creates a central repository of data, a data warehouse.

   The data warehouse stores all data in one place where the data is easily accessible. It is essential for the automatic creation of real-time data dashboard that allows the district to operate more effectively and enable teachers and administrators to pinpoint and concentrate on improving certain areas of student achievements.

VII. Cybersecurity:

With the district's increase usage of technology and proliferation of digital threats from inside and outside of the district's network, the district created an Information Security Advisor position, now Information Security Manager, that directly reports to the Chief Information Officer. The primary responsibility of the Information Security Manager is to ensure all FBISD technology processes, equipment, practices, and environment are secured and follow industry best practices in information security. The Information Technology Division continues proactive internal and external vulnerability scanning of all critical systems to ensure the systems are properly configured and patched. This activity complements on-going efforts to harden and secure workstations and servers following industry best practices and utilizing secure operating system builds.

Several security systems were deployed or are planned for future deployment contingent upon sufficient funding. A security platform was implemented to detect and minimize the impact of ransomware if an outbreak were to occur. Another system ensures two-factor authentication for employees to safely connect to their PeopleSoft payroll and other sensitive information.

Achieving compliance with recently passed Texas House and Senate bills is a primary goal for FBISD Information Technology Division:

- HB3834 requires school districts to implement annual security awareness training for all employees
- SB820 requires school districts to adopt a cybersecurity policy and designate a cybersecurity coordinator

With the passage of SB820 and HB3834, school districts are required to implement security measures, policies, and procedures to protect students' data. To adhere to Texas SB820, proper IT cybersecurity solutions are needed to ensure IT infrastructure is secure and all student personal identifiable information (PII) is protected. The District has developed and implemented district-wide cybersecurity policy to protect the confidentiality, integrity and availability of sensitive data. The Texas Cybersecurity Framework (TCF), developed by Texas Department of Information Resources (DIR), provides the guidelines for TX State agencies, including TX school districts, to follow. The TCF details the functions and objectives that are designed to protect school districts' that include identification of information asset, asset access control, and detection of vulnerabilities in addition to response to incidents and recovery from a disaster (such as a breach). It is important to note that though the legislature now requires these cybersecurity solutions, funding was not provided, making this an unfunded mandate. FBISD's Information Security Plan follows the Texas Cybersecurity Framework (TCF) which is comprised of 46 controls (such as "Information Security Risk Management" and "Malware Protection") aligned with five core functions (Identify, Protect, Detect, Respond and Recover). This layered approach is critical to identify risks and threats and ensure we are prepared to respond and recover from a breach or attack. The cyber threat landscape continues to expand and accelerate, and K-12 institutions are highly targeted because historically they are underfunded and understaffed with regards to cyber security tools and analysts.

Expanding FBISD detection capabilities (intrusion detection, behavioral anomalies), protection capabilities (end point protection, enhanced email protections) and most importantly FBISD's response capabilities (dedicated cyber analysts, after-hours responders) are key cyber security goals for the upcoming school year. Detection capabilities include software applications and tools that meet the minimum cybersecurity needs under SB820. However, the district currently has increased the number of network-connected devices to more than 60,000 due to the online instructional model implemented for COVID-19. It is anticipated that the current level of technology utilization in the District will continue, resulting in the need for additional security platforms to protect the district's network. The additional software applications, tools, and staffing will move the district beyond the minimum level of safety, better protecting data associated with students and staff. Since many of the cybersecurity monitoring tools are service based, these services cannot be funded through Bond funds and instead will be added as opportunities to pursue should expanded General Fund resources become available to accommodate these needs.