Mabank ISD

Technology Policy

Adopted 2-8-2024 by MISD Tech Dept. and Superintendent

Approved 2-26-2024 by MISD Board of Trustees

Enacted in accordance with the SB820 Mandate

Table of Contents

Introduction and Explanation

Why this policy?

Mabank ISD uses technology in almost every facet of its day-to-day activities and infrastructure. It is more important than ever before to establish policies and norms for secure technology use that implement best practices and procedures supported and maintained by the National Institute of Standards and Technology and other comparable school districts within Texas. Texas Senate Bill 820 also calls for school districts to adopt such a policy. Therefore, this serves to meet that mandate as well.

Definition of Committee Involved

The Mabank ISD Technology Policy Committee is comprised of the following participants who have drafted and approved this document for presentation to the Mabank ISD Superintendent and Board of Trustees:

David Glosup (Director of Technology)
Karen Grisham (Administrative Assistant to Technology Director)
Bobby Dillingham (Network Technician)
Rhonda Manning (Technologist)
Chelsey Richards (CTE IT Instructor)

Ratification Procedures:

The Mabank ISD Technology Policy Committee will meet no less than 3 times yearly to draft, revise, and finalize this document. It will then be presented to the Superintendent for approval. Upon approval and/or revisions requested, a final copy will be presented to the Board of Trustees at which time the policy will be ratified and published on the Mabank ISD Technology Department website.

District Technology Vision

Mabank ISD is committed to utilizing technology in a productive and engaging manner that puts a priority on both student needs as well as efficiency, practicality, and safety. With that said, the Mabank ISD Technology Department operates on an implicit deny policy regarding device, filter and firewall procedures. This means that devices, websites, and other technological avenues belonging to questionable categories are blocked off until requested to be opened. If the Technology Department finds the access request to be legitimate to educational needs, safe for the Mabank ISD network, and practical in its application coupled with existing technology components, the request will be granted. This vision and procedure by itself sets a great foundation for cybersecurity in our district. More detailed policies and procedures are found in the following pages.

Technology Department Policies

Help Desk Support Policies

The Mabank ISD Technology Department prides itself in providing quality timely service to staff and students in need of technology help throughout the district. In order to best service the needs of all, we require the following in regard to gaining assistance:

- **Technology Request:** The Technology Department asks that anyone needing help submit a technology request by either clicking the icon titled “MISD Tech Request” (icon looks like a computer monitor with speech balloon attached) or by clicking the link on the district website under “Faculty and Staff” that says “Technology Request”.
- We require that individuals submit their own technology requests and not reach out to others to do it for them. This eliminates unnecessary middle man traffic and helps to resolve issues at the source.
- **Exception:** If an individual is locked out of their google account and cannot access the portal and/or does not have internet, they may reach out to the nearest individual with access to submit a request for them.
- Technology Requests allow the Technology Department to make sure that all requests are accounted for and attended to. It also documents changes made and procedures implemented to resolve different issues. These documentations can be used later by the Technology Department to resolve similar issues.
- **Important:** Only staff are permitted to submit technology requests. Students needing assistance should have a staff member submit a request for them.

Technology Facility/Room/Closet Policies:

The Mabank ISD Technology Office is open Monday-Friday 7:45am-4:15pm on all official Mabank ISD school days. The Tech Department has personnel housed at the Administrative Office that are dispatched by Technology Administrators to tech requests coming from any campus. Individuals visiting the Technology Office should enter through the main Technology Room if they need assistance as the network technician’s office houses the Demarc and MDF for the building and needs to remain secure. All District MDF and IDF closets are to remain locked at all times. Only technology equipment should be stored in district MDF and IDF closets.

Disaster Recovery Plan and Procedure

Mabank ISD has taken many steps to mitigate the negative technological results of a disaster. The district stores as much data as it can in the cloud via Region 10, ISCorp or other hosted services. This move is in conjunction with many other districts of similar size in the region and has proven highly successful.

In the event of a disaster that renders facilities unuseable, Mabank ISD would reach out to Region 10 ESC, ISCorp, Zayo, and Cynergy Technology to restore our network backbone. At that point, 95% of services would be accessible by district staff and students. Due to storage and financial limitations, the only critical data stored onsite that is not backed up is surveillance footage.

Private Cloud/BaaS With Region 10:

To further explain the cloud hosting at Region 10, Mabank maintains a direct circuit 10GB connection to Region 10 via Zayo WAN services. Because of this high speed connection, Mabank ISD benefits from Region 10's robust data center and network infrastructure while still acting as if the servers are on-premise. Engineers at Region 10 have quick access to Mabank ISD's server infrastructure to help spin up new virtual machines, provide routine maintenance, and assist in condensing and/or retiring older servers. These services include the following features:

- 10GB EVC (Ethernet Virtual Circuit) provides layer 2, high bandwidth/low latency connection between Mabank ISD data center and the Region 10 data center.
- All Mabank ISD workloads on R10 Private Cloud VMware cluster, which guarantees high availability from server or storage failures.
- Workloads run in an all-flash environment – very high performance.
- Mabank ISD has access to the vSphere web interface to manage VMs at the hypervisor level.
- Mabank ISD servers are backed up daily and stored at R10's DR site at Infomart. R10 keeps 8 daily, 5 weekly, and 3 monthly for each workload. Backups are encrypted. R10 keeps 7 daily backups on immutable storage. Nightly backups are stored off-site and, more importantly, off-network at Region 10. In the event Mabank ISD's Veeam environment was compromised, the "air-gapped" technology built into Veeam's Insider Protection feature for Service Providers ensures an attacker cannot erase or corrupt the backup sets already at Region 10. Both Private Cloud and BaaS offerings guarantee the safety of Mabank ISD's data. With

Private Cloud, it is trivial to almost immediately restore all of Mabank ISD's workloads from a time before the hacking event took place (through storage snapshots). If R10 ever did have to restore from backup, Private Cloud guarantees a safe place for those backups to land to get Mabank ISD's services up with minimal downtime.

- Hourly storage array snapshots of Mabank ISD servers with the ability to roll back to a particular point in time in less than a minute.
- Mabank has provisioned a true disaster recovery site by replicating workloads to Infomart in Dallas. In the case of a site outage at the Spring Valley production site, all server workloads can be spun up at Infomart with the assistance of R10 engineers.
- Primary and secondary data centers that are protected by large battery backup and diesel generators.
- Enterprise-level server EDR security endpoint client for all Mabank ISD server workloads.
- R10 best practice management of Mabank ISD virtual machines along with detailed monitoring and alerting.
- During the migration to R10, R10 became familiar with the Mabank ISD environment and worked to remediate any architecture or other issues that were uncovered.
- Windows Updates maintenance and Windows Server upgrades to new versions are performed by R10.
- Four experienced K12 R10 network and security engineers who are available to assist with any enterprise or security issues that arise.
- R10 handles enterprise servers and storage lifecycle management.
- R10 handles all server and storage performance, maintenance, hardware or software upgrades, etc.
- All hypervisor updates, security concerns, and management performed transparently by Region 10.
- Veeam licensing or support.
- Backup storage, its lifecycle management and replacement.
- Building an effective disaster recovery site for Mabank is baked into the solution at R10.
- R10 has an environment engineered from the ground up focused on high-availability, performance, data security.

ISCorp Student Information System Hosting

ISCorp is Skyward's trusted partner in hosting and provides all updates, maintenance, and addendums to Mabank ISD's student information system. ISCorp support is very responsive in the event of trouble and quickly communicates in the event of outages. The services include the following features:

- Dual-Redundant Firewalls, BGP Failover, Antivirus Scanning and Mitigation.
- 24x7 Infrastructure Monitoring and Alarming.
- Progress Database Administration.
- 7am – 7pm (Central Time) Support.
- Daily Backups Stored Offsite.
- RTO 72 hrs max RPO 72 hrs max
- HIPAA Certification

Scinary Cybersecurity Services

In regard to cybersecurity attacks specifically, Mabank ISD contracts with Scinary Cybersecurity to identify and resolve threats. They provide both a Security Information/Event Management and Intrusion Detection System. Their appliance sits inside Mabank ISD's network right after the firewall. The services include the following features:

- Rules-based Network Security Appliance designed to be both a SIEM and IDS.
- Works by reviewing all of Mabank ISD's network traffic that passes through the firewall.
- Analyzes traffic and matches it to the ruleset. If there is a match, an alert is issued to the Director of Technology and Network Technician with steps to resolve.
- Viruses and Malware can often trick or disable traditional AV, before infecting computers. Scinary looks for that activity.
- End-Users are Mabank ISD's biggest risk. Scinary analyzes the websites and downloads that come through the network and alerts Mabank ISD to suspicious traffic.
- In case of an incident or data breach, Scinary keeps the traffic for future analytics if needed.
- Scinary works with Mabank ISD to develop a Cybersecurity Framework on a yearly basis that accompanies this policy.
- Region 10 also alerts the district of global account breaches with steps to resolve.

Staff Technology Policies

Staff Onboarding/Offboarding Policies:

All staff upon entering the district receive a login for district computers, a district email account, a district google account, and ClassLink account. (ClassLink includes Skyward Gradebook and Employee Access.) All of these accounts are district owned and are subject to query at the request of Mabank ISD Administration and/or open records request by an individual with respect to federal, state, local and TEA requirements. Please review Appendix 1 for more information regarding acceptable use of district accounts and resources. The district retains account activity for staff who resign or are terminated for a maximum of 6 months.

Staff Password Policies:

Upon entering the district, staff are given a temporary password that is to be reset as soon as possible to a complex password meeting the following requirements:

- At least 8 characters in length
- Use of at least one special symbol (i.e. $, #, @...)
- Use of at least one number (i.e. 1, 2, 3, 4…)
- Use of different cases (i.e. A, a, B, b…)
- Discouraged use of full words (i.e. texasisawesome1200)
- Discouraged use of names (i.e. annieiscool1234)
- Discouraged use of familiar public dates (i.e. anniversaries, graduation dates, etc.)
- Encouraged use of random number, special character, and different cases…the stranger and more complex, the better!
- Under no circumstances are staff passwords to be shared with anyone in any way, shape, or form. Technicians needing to help staff will reset their passwords for the extent of the help and reset them again once work is completed.

Technology Purchasing Policies:

Any and all technology purchases must be cleared through the Mabank ISD Technology Department before moving forward. Network and device requirements must be analyzed and approved for activity on the Mabank ISD network. Any staff member wanting information on purchasing new technology or upgrading/replacing older technology needs to contact their administrator and the Technology Department for options and quotes. Buying and/or bringing any technology into Mabank ISD without the notification and approval of the Mabank ISD Technology Department and the campus administrator is a violation of standards and procedures outlined in this document and will be dealt with in a disciplinary fashion that is fitting to the offense.

Student Technology Policies

Student Onboarding/Offboarding Policies:

All students upon entering the district receive a login for district computers, a district google account, and ClassLink account. (ClassLink includes Skyward Student Access for Junior High and High School students.) All of these accounts are district owned and are subject to query at the request of Mabank ISD Administration and/or open records request by an individual with respect to federal, state, local and TEA requirements. Please review Appendix 1 for more information regarding acceptable use of district accounts and resources. The district retains account activity for students who leave the district for a maximum of 3 months.

Students have access to email accounts according to the following guidelines:

- Students grades 9-12 have access to email accounts with the ability to email internally and externally.
- Students grades 5-8 have access to email accounts that are locked down to only send/receive emails from SchoolMessenger in order to be able to do account maintenance on their SchoolMessenger accounts. (i.e. reset password, etc.)

Student Password Policies:

Student passwords at the 5th-12th grade level are set uniquely by the students with the following complexity requirements:

- At least 8 characters in length
- Use of at least one special symbol (i.e. $, #, @...)
- Use of at least one number (i.e. 1, 2, 3, 4…)
- Use of different cases (i.e. A, a, B, b…)
- Discouraged use of full words (i.e. texasisawesome1200)
- Discouraged use of names (i.e. annieiscool1234)
- Discouraged use of familiar public dates (i.e. anniversaries, graduation dates, etc.)
- Encouraged use of random number, special character, and different cases…the stranger and more complex, the better!

Student passwords at the Below Kindergarten-4th grade level are set to random complex strings and these students are given QR code quickcards to login with day to day.

Technology Equipment Policies

Storage:

Mabank ISD is not responsible for data saved to hard drives on individual computers. ***All Staff and Students*** are encouraged to backup ***all*** important data to their district Google Drive as well as two other separate storage mediums. (i.e. external hard drive, personal Google drive, flash drive, other personal cloud storage, etc.)

- Mabank ISD's Student Information System (Skyward) is hosted with ISCorp who provides redundancy and backups for that platform
- All of Mabank ISD's servers with the exception of camera servers are housed and backed up up by Region 10 Education Service Center

Printers:

Mabank ISD installs mostly HP laser printers but the district is moving in the direction of replacing many printers with fewer copiers. The district does not support personal inkjet printers. If a staff member brings an inkjet printer that is plug-and-play and it works when plugged into the computer via USB, they may use it. However, the technology dept. will not provide support for said printer nor will district funds be used to purchase ink for it.

Other Technology Equipment:

- Mabank ISD students are provided chromebooks to do their work with by the district. Therefore, students are not permitted to bring technology devices of their own.
- Staff are permitted to use their own computer peripherals. (wireless mice, keyboards, clickers, etc.) Under no circumstances is a staff member to bring any of the following devices as they could greatly damage the network or are not compliant with district policies:
    - Home Wireless Routers
    - Switches
    - Cell Phone Jammers
- Educators are provided one large format display per classroom. This can be a Smart Interactive Board (requiring projector), a non-interactive television or an interactive flat panel television.

Annual Technology Evaluation Procedure

2023-2024 Year Evaluations/Implementations

The Mabank ISD Technology Department has taken several measures this year to improve cybersecurity throughout the district including:

- Updated and Revised Technology Policy including cybersecurity objectives, district technology procedures and state required cybersecurity framework.
- All educators required to take Region 10's DIR Approved Cybersecurity Training.
- Changed the remote access password for all nodes to a more complex and secure one.
- Encouraged staff to use Windows + L to lock their screens when they step away from their computer.
- Moved Firewall services to Region 10 ESC saving the district money as well as providing a more redundant and stable firewall solution.
- Replaced battery backups district wide and implemented an ad hoc generator solution at the administrative hub to keep the internet on in case of power outages.
- Implemented 2-Factor Authentication for all staff accounts including ClassLink, Skyward, Email, and Google
- Mandated all students 5th-12th grade set their own complex passwords
- Mandated use of QR codes with complex unknown passwords for all Below Kindergarten-4th grade students.
- Addition of PF360 cloud printing via copy machines leased from Ubeo. This allows staff to securely print jobs to a cloud repository that can be retrieved at any of the copiers district wide. The job does not physically print until the staff member authenticates via a numeric code into the copier and selects the job.
- Upgraded all existing campus signs including removal of outdated and vulnerable computers that ran original signs.

Mabank ISD
Acceptable Use Policy

Purpose

The Mabank Independent School District furnishes an array of technology resources in order to advance its vision for 21st century learners. The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes. Resources include, but are not limited to, the Internet, system network, personal computers, mobile devices, telecommunication tools, and educational software. All users – students and staff – are expected to exercise sound judgment and personal responsibility in the use of district resources. The District's policies, guidelines, support, and training are intended to promote an effective, safe, productive, and instructionally sound educational environment.

Availability of Access

Access to the District's Electronic Communications System is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies (See TASB Policy DH, FNC, FNCJ, FO, and the Student Code of Conduct). **Any user identified as a security risk or having violated District and/or campus computer-use guidelines may be denied access to the District's system.** Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Administrative Regulations for Electronic Communication and Data Management

The District's system will be used only for administrative and educational purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.
Copyrighted software or data may not be placed on any system connected to the District without permission from the holder of the copyright. Only the owner(s), or individuals specifically authorized by the owner, may upload copyrighted material to the system.

Disclaimer of Liability

The District shall not be liable for user's inappropriate use of electronic communication resources or violations of copyright restrictions, user's mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet.

Monitored Use

Use of all district resources and electronic mail transmissions by students and employees should not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use for educational or administrative purposes.

Individual User Responsibilities (Acceptable Use)

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements, consistent with the purposes and mission of the District and with law and policy governing copyright. (See TASB Policy FNCE) The MISD reserves the right to inspect and/or remove data, email, or files without prior consent of system users.

The following standards will apply to all users of the District's electronic information/communications systems:

- The individual in whose name system accounts are issued shall be responsible at all times for its proper use.
- Users may not access or employ another person's system account without written permission from the campus administrator or district coordinator, as appropriate.
- Users may not engage in searching, viewing, or uploading any content that is offensive, pornographic, or connected to illegal activity. Unintended connection to prohibited content should be reported to the appropriate teacher or supervisor immediately.
- System users are expected to abide by all copyright laws and regulations. Users may not possess, share, or redistribute unauthorized, copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the terms of use or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations. System users are responsible for determining whether a program is in the public domain.
- System users are expected to refrain from plagiarism and shall properly cite sources.
- Users are allowed limited personal use of technology resources as long as it does not interfere with or burden the district's educational mission.
- The MISD is not responsible for loss of data or files. It is the responsibility of individual users to backup files to an external hard drive or server.
- Users are not permitted to utilize the district's system for gaming, instant-messaging, social networking, or to download or stream personal music or videos.
- Where music or videos are necessary to support educational goals, users should take measures to avoid live streaming, which places a burden on the system.
- Any downloads should be pre-approved and should support the district's educational mission.
- District resources may not be used for private or monetary gain.
- Users should not use the district's system to forward personal, political, religious, or objectionable content.
- Users should never attempt to circumvent the district's filtering software to access objectionable material or to encrypt communication to avoid review.
- Paid streaming applications are blocked with the exception of YouTube per executive administration.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution of costs associated with system restoration, hardware, or software costs.

Forgery Prohibited

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited. Attempts may lead to possible disciplinary action.

Information Content/Third Party Supplied Information

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems on the global electronic network that may contain inaccurate and/or objectionable material.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privilege on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

Network Etiquette

System users are expected to observe the following network etiquette:

- Use of the District's network or systems is intended for educational purposes only.
- The District's network is a non-private entity. Users should remain mindful that all activity can be viewed globally and will leave a digital footprint.
- All users are expected to maintain appropriate network decorum.
    - Never send, or encourage others to send abusive messages. Inappropriate language -- profanity, vulgarity, use of ethnic or racial slurs, and any other inflammatory language -- is prohibited.
    - Transmitting obscene messages or pictures is prohibited.
- At no time should use of the network create a disruption to the District's educational mission.
- Respect privacy. Revealing others' personal addresses, phone numbers, user IDs, passwords, or files is prohibited.
- Any data or communication placed on district equipment will become the property of Mabank ISD.

Electronic Mail Guidelines

The software and hardware that provides district email capabilities has been publicly funded and should not be considered a vehicle for private, personal communication. **The content of all district email communication is governed by the *Open Records Act*. The Mabank ISD will cooperate with and abide by any legal request for access to email contents by the proper authorities.**

Email access is provided as a normal operating tool for any employee to perform their job. Individual staff email addresses will be shared with interested parents and community members who request to communicate with staff for educational purposes. Email addresses are made public through the campus web page.

System users must purge electronic mail in accordance with established retention guidelines.
Employees are expected to return email communications to parents or other public members who have a legitimate business requests within 24 hours whenever possible. Requests for information from outside agencies should be handled in a manner consistent with previous experience in working with similar requests.

Requests for staff or students' personal information should not be honored via email.

- It is critical for a personal contact to be made with any individual requesting personal information. This relates particularly to any requests for student grades, discipline, attendance, enrollment status, dates of birth, photos or other likenesses, or related information. In addition, security information such as username or password should not be sent via email for any reason.
- Employee management of student information must comply with the *Family Educational Rights and Privacy Act (FERPA)*.

Principal approval is required before sending messages to an entire campus.

Superintendent approval is required before sending messages to the entire district.

Do not forward messages that have no educational or professional value.

Never open attachments from unknown sources.

- Attachments to email messages should include only data files. At no time should program files (typically labeled ".exe") be attached.
- Program files received as attachments over the Internet may include viruses or other very destructive capabilities once they are executed. Delete such email message immediately without saving or looking at the attachment.

Email format should include a signature footer including name, position, affiliation, and internet address (if applicable).

Messages relating to or in support of illegal activities must be reported to the authorities. Impersonating others is considered inappropriate.

Blogging

Any blog that creates a material or substantial disruption to the educational environment, regardless of the origin of the blog, is prohibited. Situations that may amount to a material and substantial disruption include but are not limited to:

- A published threat toward a student, teacher, administrator, or other school employee.
- Blog postings that call for the violation of laws or school rules.
- Staff or students who post on their personal blogs during school time.
- Students who use school resources to publish or view a blog that is not school sponsored.
- Publishing false statements or rumors about others that can damage reputations and lead to defamation of character.

MISD Consequences

Student violation of Acceptable Use policy may result in disciplinary action, including but not limited to the following:

- Loss of computer or network privileges. Duration shall be set by the building Principal in collaboration with the Director of Technology.
- Detentions

- In-School Suspension
- Suspension
- DAEP Placement
- Expulsion
- Financial responsibility for all costs associated with system restoration, including labor, hardware or software repair/replacement, and restoring the integrity of data.
- Criminal charges

Termination/Revocation of System User Account

The District may suspend or revoke any system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.
Termination of employee's account or of a student's access will be effective on the date the Principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The district does not warrant that the functions of services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.
The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's Electronic Communication System.

Revised December 2023