TECHNOLOGY PLAN

Revised 2023

Summersville R-II School District

Table of Contents

Technology Plans/Policies

I. District Mission Statement

The mission of the Summersville R-II School District is to direct each student's learning so that he/she can become a productive citizen in our changing world.

II. District Educational Philosophy

Education is a lifelong process during which each student develops at an individual rate in physical, mental, social, emotional, and academic areas.

The primary objective of our school is the growth and development of the individual in ways that will help him/her become a well-adjusted contributing member of society. The Summersville R-II Board of Education believes the home, school, and church all play an important role this development.

Education is the major responsibility of the school. We expect our students to master the essential skills of education. These skills will prepare them to become lifetime learners.

We believe education is a privilege. Inherent in this belief is the development of respect for self and others, rights and responsibilities of citizenship, and a desire to learn and achieve in authentic ways.

III. District Educational Objectives

It is the belief of the Summersville R-II School District that one of the fundamental rights of each individual is the right of equal access to educational opportunities regardless of race, creed, or socio-economic status. Each learner receiving these guaranteed rights will have the opportunity to develop intellectually, emotionally, physically and socially to the best of his/her ability as a lifetime learner.

1. Our learners will acquire the knowledge and skills to:
    - Gather, analyze, and apply information and ideas.
    - Communicate effectively within and beyond the classroom.
    - Recognize and solve problems
    - Make decisions and act as responsible members of society.
    - Develop and maintain a positive self-image.
2. Our district will emphasize and is committed to:
    - Parental and community involvement
    - Challenging and diversified instructional programs.
    - A safe and non-threatening environment.
    - Professional faculty and staff.

- An atmosphere conductive to learning
- Positive work ethics.
- Cooperative interrelationships.

IV. CSIP Goals/Objectives

1. **75% of the district's students will score in the proficient and advanced levels on the MAP.**
   1.1. District curriculum will be aligned with the frameworks and Show-Me Standards
   1.2. Lesson Plans and testing procedures will model MAP testing.
   1.3. Schedules and teaching assignments will be adjusted based on the analysis of MAP data
   1.4. MAP incentives and accountability methods will be developed and communicated to students
   1.5. The district will provide instruction and guided practice on test-taking skills to all students.
   1.6. The district will provide professional development opportunities that focus on district-wide improved teaching strategies and techniques that support improved student achievement.
2. **The district will increase ACT test scores to meet or exceed state and national averages.**
   2.1. The district will develop policies which encourage student participation in ACT testing program.
   2.2. The district will analyze and revise curriculum to ensure ACT standards are included.
   2.3. Teachers will receive professional development regarding ACT test
3. **District reading performance will improve and at least 85% of the students will be reading at the proficient level on MAP and/or at grade level**
   3.1. Accelerated Reading will be included in district communication arts curriculum.
   3.2. A balanced literacy program will be included in district communication arts curriculum.
   3.3. Reading intervention strategies will be available to students not reading at grade level.
   3.4. Library Media Centers will meet desired standards K-12.
4. **The district will improve the writing skills of all students in grades K -12.**
   4.1. Lesson plans will incorporate writing events at all grade levels on a regular basis.
   4.2. Professional Development activities and in-service will focus on writing
5. **The vocational program at Summersville R-II will meet all state standards and will produce graduates who are equipped to enter the world of work.**
   5.1. Increase enrollment in FACS classes.
   5.2. Add an additional vocational program to existing curriculum.
   5.3. Establish and obtain approval for state business and agriculture internship programs.
   5.4. Increase student participation in vocational organizations.

6. **The district will support the goals of the A+ program and the performance standards by instituting programs and policies which support those goals.**
   - 6.1. The district will evaluate and revise the at-risk program which includes at-risk process, advisor/advisee program and alternative school.
   - 6.2. The district will evaluate and update the four-year planning process.
   - 6.3. The district will provide career materials and career events to facilitate career planning for all students in grades K-12
   - 6.4. The district will review and increase as needed dual credit courses and articulation agreements.
   - 6.5. The district will review attendance policies and examine procedures to increase district attendance.
7. **The district will evaluate course offerings and scheduling K-12 and develop programs which meet the educational needs of all students.**
   - 7.1. The district will examine the benefits of the 10-block schedule.
   - 7.2. The elementary schedule will be revised to provide additional courses needed.
   - 7.3. The district will examine advanced courses enrollment and develop action plans to increase enrollment.
   - 7.4. Initiate plans to institute an Early Childhood Program at Summersville.
8. **The district will provide effective instructional programs and quality teachers in an environment conductive to learning**
   - 8.1. The Performance Based Teacher Evaluations will be reviewed and revised based upon current requirements and assessment data.
   - 8.2. Teachers will receive professional development pertaining to effective teaching methods.
   - 8.3. The district technology will support the educational process.
   - 8.4. The district will emphasize teacher recruitment as a high priority.
9. **The district will promote a safe and healthy lifestyle for the students, faculty and staff.**
   - 9.1. The district will provide a full-time nurse to be shared between the elementary and the high school.
   - 9.2. Students and faculty will receive instruction regarding safe and drug free education.
   - 9.3. The district will provide a safe environment for elementary students during after school grant program.
   - 9.4. The district will provide a safe and healthy environment for preschool age children not to exceed license requirements.
   - 9.5. The district will implement a new comprehensive health program in grades K-6
   - 9.6. The district will schedule through St. John's Employee Assistance services a workshop that deals with stress management.
   - 9.7. During school the school nurse and school counselors will provide resources for mental health concerns.

V. Technology Mission Statement

The Summersville R-II School District is committed to equipping its students with the necessary skills to be lifetime learners. To accomplish this goal, students must develop skills that allow them to utilize advanced technology which affects every facet of their lives. This is a reflection of our **District Goal and Objectives, District Mission Statement, and CSIP Goals** stated above.

Therefore, it is important that we direct the use of technology into the five areas listed below.

1. Student learning as it relates to the Show Me Standards, including technology skills
2. Teacher preparation and delivery of instruction
3. Administration/data management/communication processes
4. Resource distribution and use
5. Technical Support

Upon completion of a directed course of study, students can enter society as a productive member with the freedom to pursue whatever life goals they desire. **(As also stated in our District Mission Statement)**

VI. District Technology Goal

Technology must not be viewed as an end in itself. Technology is only valuable and efficient if it provides a means of accomplishing or supplementing the overall goal of education and the strengths and weaknesses as defined in the district CSIP Plan. We believe that technology in education is justified in two major areas:

1. It must prepare students for the workforce. (CSIP 1, 2, 3, 4, 5)
2. It must provide a means to make the educational process more efficient. (CSIP 6, 7, 8, 9)

With this in mind, the Summersville R-II School District sees the following as objectives for the efficient use of technology in this district:

VII. Technology Objectives

1. Enable students to use technology to acquire and manipulate information.
2. Enable students/staff to use technology as a tool for exploration and continued learning
3. Provide students with the opportunity to explore and experience existing and emerging technologies.
4. Provide appropriate technologies to students as all grade levels.
5. Provide up-to-date technologies in sufficient quantities for all students and staff.
6. Provide adequate training and encouragement to allow staff and students to effectively use available technology
7. Provide opportunity for public awareness of the need for and uses of technology in the school environment

8. Integrate technology into all areas of the curriculum
9. Provide an adequate background in technology-based application so the student will be able to use these applications to meet the challenges of today and the future.

VIII. District Curriculum Integration

Level I (Grades K-3)

- Keyboarding Strand
  - The student will develop touch keyboarding skills---second and third grades.
- Computer Literacy Strand
  - The student will explore computer technology
- Application Strand
  - The student will explain/perform computer operations
  - The student will perform word processing activities –third grade
  - The student will perform presentation/multimedia activities –third grade
- Technology and Society Strand
  - The student will explore the concepts of computer ethics.

Level II (Grades 4-6)

- Keyboarding Strand
  - The student will apply intermediate keyboarding skills.
- Computer Literacy Strand
  - The student will explore issues related to technology
- Application Strand
  - The student will perform word processing activities.
  - The student will perform telecommunication activities.
  - The student will perform presentation/multimedia activities
- Technology and Society Strand
  - The student will examine problems concerning computer ethics.

Level III (Grades 7-12)

- Keyboarding Strand
  - The student will apply advanced keyboarding skills.
- Computer Literacy Strand
  - The student will explore and apply computer concepts to classroom problems.
- Application Strand
  - The student will perform word processing activities.
  - The student will perform spreadsheet activities.
  - The student will perform database activities.

    - The student will perform desktop publishing activities.
    - The student will perform presentation/multimedia activities.
- Technology and Society Strand
    - The student will apply ethics to classroom situations.
    - The student will utilize technology to reinforce classroom learning.

Students will master these competencies through regular classroom activities, integrating technology into the classroom curriculum.

IX. POLICIES

A. Technology Usage Policy (EHB)

The Summersville R-II School District's technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Research shows that students who have access to technology improve achievement. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the district, all of which positively impact student achievement. The district will periodically conduct a technology census to ensure that instructional resources and equipment that support and extend the curriculum are readily available to teachers and students.

The purpose of this policy is to facilitate access to district technology and to create a safe environment in which to use that technology. Because technology changes rapidly and employees and students need immediate guidance, the superintendent or designee is directed to create procedures to implement this policy and to regularly review those procedures to ensure they are current.

1. Definitions

For the purposes of this policy and related procedures and forms, the following terms are defined:

Technology Resources – Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; audio-visual equipment; Internet; electronic mail (e-mail); electronic communications devices and services, including wireless access; multi-media resources; hardware; and software. Technology resources may include technologies, devices and services provided to the district by a third party.

User – Any person who is permitted by the district to utilize any portion of the district's technology resources including, but not limited to, students, employees, School Board Members and agents of the school district.

User Identification (ID) – Any identifier that would allow a user access to the district's technology resources or to any program including, but not limited to, e-mail and internet access.

Password – A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

2. Authorized Users

The district's technology resources may be used aby authorized students, employees, School Board Members, and other persons approved by the superintendent or designee, such as consultants, legal counsel and independent contractors. All users must agree to follow the district's policies and procedures and sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless excused by the superintendent or designee.

Use of the district's technology resources is a privilege, not a right. No potential user will be given an ID, password, or other access to district technology if he or she is considered a security risk by the superintendent or designee.

3. User Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources including, but not limited to, voicemail, telecommunications, email and access to the internet or network devices. By using the district's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by the district. A user ID with email access will only be proved to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received, or stored using district technology.

Electronic communications, downloaded material and all data stored on the district's technology resources, including files deleted from a user's account, may be intercepted, accessed, monitored, or searched by district administrators or their designees at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with district policies and rules and investigating potential misconduct. Any such search, access or interception shall comply with all applicable laws. Users are required to return district technology resources to the district upon demand including, but not limited to, mobile phones, laptops, and tablets.

4. Technology Administration

The Board directs the superintendent or designee to assign trained personnel to maintain the district's technology in a manner that will protect the district from liability and will protect confidential student and employee information retained on or accessible through district technology resources.

Administrators of district technology resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies and

procedures. All district technology resources are considered district property. The district may remove, change, or exchange hardware or other technology between buildings, classrooms or users at any time without prior notice. Authorized district personnel may install or remove programs or information, install equipment, upgrade any system, or enter any system at any time.

5. Content Filtering and Monitoring

The district will monitor the online activities of minors and operate a technology protection measure ("content filter") on the network and all district technology with Internet access, as required by law. In accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography. Content filters are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by the district is prohibited.

The superintendent, designee or the district's technology administrator may fully or partially disable the district's content filter to enable access for an adult for bona fide research or other lawful purposes. In making decisions to fully or partially disable the district's content filter, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

The superintendent or designee will create a procedure that allows students, employees, or other users to request that the district review or adjust the content filter to allow access to a website or specific content.

6. Online Safety, Security and Confidentiality

In addition to the use of a content filter, the district will take measures to prevent minors from using district technology to access inappropriate matter or materials harmful to minors on the Internet. Such measures shall include, but are not limited to, supervising and monitoring student technology use, careful planning when using technology in the curriculum, and instruction on appropriate materials. The superintendent, designee and/or the district's technology administrator will develop procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.

All minor students will be instructed on safety and security issues, including instruction on the dangers of sharing personal information about themselves or others when using e-mail, social media, chat rooms or other forms of direct electronic communication. Instruction will also address cyberbullying awareness

and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

This instruction will occur in the district's computer courses, courses in which students are introduced to the computer and the Internet, or courses that use the Internet in instruction. Students are required to follow all district rules when using district technology resources and are prohibited from sharing personal information online unless authorized by the district.

All district employees must abide by state and federal law and Board policies and procedures when using district technology resources to communicate information about personally identifiable students to prevent unlawful disclosure of student information or records.

All users are prohibited from using district technology to gain unauthorized access to a technology system or information; connect to other systems in evasion of the physical limitations of the remote system; copy district files without authorization; interfere with the ability of others to utilize technology; secure a higher level of privilege without authorization; introduce computer viruses, hacking tools, or other disruptive/destructive programs onto district technology; or evade or disable a content filter.

7. Closed Forum

The district's technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law. The district's web page will provide information about the school district but will not be used as an open forum.

All expressive activities involving district technology resources that students, parents/guardians and members of the public might reasonably perceive to bear the imprimatur of the district and that are designed to impart knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school district for legitimate pedagogical reasons. All other expressive activities involving the district's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

8. Inventory and Disposal

The district will regularly inventory all district technology resources in accordance with the district's policies on inventory management. Technology resources that are no longer needed will be disposed of in accordance with law and district policies and procedures related to disposal of surplus property.

9. Violations of Technology Usage Policies and Procedures

Use of technology resources in a disruptive, inappropriate, or illegal manner impairs the district's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term, or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district's technology resources.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the district's technology policies and procedures. Any attempted violation of the district's technology policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation. The district will cooperate with law enforcement in investigating any unlawful use of the district's technology resources.

10. Damages

All damages incurred by the district due to a user's intentional or negligent misuse of the district's technology resources, including loss of property and staff time, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

11. No Warranty /No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis.

The district is not responsible for loss of data, delays, non-deliveries, mis deliveries or service interruptions. The district does not endorse the content nor guarantee the accuracy or quality of information obtained using the district's technology resources.

B. Technology Usage – Technology Safety (EHB-AP-1)

1. Student Users

All student users and their parents/guardians must sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless otherwise excused by this policy or the superintendent or designee. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign or consent to the User Agreement without additional signatures. Students who do not have a User Agreement on file with the district may be granted permission to use the district's technology resources by the superintendent or designee.

2. Employee Users

No employee will be given access to the district's technology resources unless the employee agrees to follow the district's User Agreement prior to accessing or using the district's technology resources. Authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policies or procedures, hinder the use of the district's technology resources for the benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology resources or interferes with the effective and professional performance of the employee's job is considered unreasonable. Unless authorized by the employee's supervisor in advance, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.

3. External Users

Consultants, legal counsel, independent contractors, and other persons having business with the district may be granted user privileges at the discretion of the superintendent or designee after consenting to the district's User Agreement and for the sole, limited purpose of conducting business with the school. External users must abide by all laws, district policies and procedures.

4. General Rules and Responsibilities

The following rules and responsibilities will apply to all users of the district's technology resources:

a) Applying for a user ID under false pretenses or using another person's ID or password is prohibited.
b) Sharing user IDs or passwords with others is prohibited except when shared with the district's technology department for the purpose of support. Individuals who share IDs or passwords may be disciplined and will be held responsible for any actions taken by those using the ID or password. A user will not be responsible for theft of passwords and IDs but may be responsible if the theft was the result of user negligence.
c) Deleting, examining, copying, or modifying district files or data without authorization is prohibited.
d) Deleting, examining, copying, or modifying data belonging to other users without their prior consent is prohibited.
e) Mass consumption of technology resources that inhibits use by others is prohibited.
f) Use of district technology for soliciting, advertising, fundraising, commercial purposes or financial gain is prohibited, unless authorized by the district or in accordance with policy KI. Use of district technology resources to advocate, support or oppose any ballot measure or candidate for public office is prohibited.
g) Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
h) Users are required to obey all laws, including criminal, copyright, privacy, defamation, and obscenity laws. The district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law.
i) The district prohibits the use of district technology resources to access, view or disseminate information that is pornographic, obscene, child pornography, harmful to minors, libelous, or pervasively indecent or vulgar.
j) Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.
k) The district prohibits the use of district technology resources to access, view or disseminate information that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g., threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and

present likelihood that, because of their content or their manner of distribution, they will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful district policies and procedures.

l) The district prohibits any use that violates any person's right under applicable laws, and specifically prohibits any use that has the purpose of effect of discriminating against or harassing any person on the basis of race, color, religion, sex, national origin, ancestry, disability, age, genetic information, pregnancy or use of leave protected by the Family and Medical Leave Act (FMLA).

m) The district prohibits any unauthorized intentional or negligent action that damages or disrupts technology, alters its normal performance or causes it to malfunction. The district will hold users responsible for such damage and will seek both criminal and civil remedies, as necessary.

n) Users may install and use only properly licensed software and audio, or video media purchased by the district or approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license and approved by the district.

o) At no time will district technology or software be removed from district premises, unless authorized by the district.

p) All users will use the district's property as it was intended. Technology resources will not be moved or relocated without permission from a building administrator. All users will be held accountable for any damage they cause to district technology resources.

5. Technology Security and Unauthorized Access

a) All users shall immediately report any security problems or misuse of the district's technology resources to a teacher or administrator.

b) Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.

c) Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.

d) The unauthorized copying of system files is prohibited.

e) Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
f) Users will be granted access privileges to district technology resources as determined appropriate by the superintendent or designee. Any attempt to secure a higher level of privilege without authorization is prohibited.
g) The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a district computer, network or any external networks is prohibited.

6. Online Safety and Confidentiality

Curricular or noncurricular publications distributed using district technology will comply with the law and Board policies on confidentiality.

All district employees will abide by state and federal law, Board policies and district rules when using district technology resources to communicate information about personally identifiable students. Employees will take precautions to prevent negligent disclosure of student information or student records.

All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are prohibited from sharing such information unless authorized by the district. Student users shall not agree to meet with someone they have met online without parental approval and must promptly disclose to a teacher or another district employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

7. Electronic Mail and Messaging

A user is generally responsible for all e-mail and other electronic messages originating from the user's accounts; however, users will not be held responsible when the messages originating from their accounts are the result of the account being hacked.

a) Forgery or attempted forgery of electronic messages is illegal and prohibited.
b) Unauthorized attempts to read, delete, copy, or modify electronic messages of other users are prohibited.
c) Users are prohibited from sending unsolicited mass email or other electronic messages. The district considers more than five addresses per message, per day a violation, unless the

communication is a necessary, employment-related function or an authorized publication.

d) When communicating electronically, all users must comply with district policies, regulations and procedures and adhere to the same standards expected in the classroom.

e) Users must obtain permission from the superintendent or designee before sending any district-wide electronic messages.

8. Communication Devices

Employees and others to whom the district provides mobile phones or other electronic communication devices must use them professionally and in accordance with district policies, regulations, and procedures. These devices shall not be used in a manner that would distract the employee or other user from adequate supervision of students or other job duties.

9. Exceptions

Exceptions to district rules will be made for district employees or agents investigating use that potentially violates the law, district policies or procedures. Exceptions will also be made for technology administrators who need access to district technology resources to maintain the district's resources or examine and delete data stored on district computers as allowed by the district's retention policy.

10. Waiver

Any user who believes he or she has a legitimate educational purpose for using the district's technology in a manner that may violate any of the district's policies, regulations or procedures may request a waiver from the building principal, superintendent, or their designees. In making the decision to grant a waiver to a student, the administrator shall consider the student's purpose, age, maturity, and level of supervision involved.

C. Data Governance and Security (EHBC)

To accomplish the district's mission and comply with the law, the district must collect, create, and store information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws mandating confidentiality, and maintaining the trust of the district's stakeholders. All persons who have access to district data are required to follow state and federal law, district policies and procedures, and other rules created to protect the information.

1. Definitions

Confidential Data/Information – Information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information – Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential.

2. Responsibility and Data Stewardship

All district employees, volunteers and agents are responsible for accurately collecting, maintaining and securing district data including, but not limited to, information that is confidential or is critical to district operations.

3. Information Security Officer

Nathaniel Karr - Technology Director is the district's information security officer (ISO) and reports directly to the superintendent or designee. The district's information security officer is directed to create and review district procedures on collecting and protecting district data including, but not limited to, securely maintaining confidential and critical information. The ISO is responsible for implementing and enforcing the district's security policies and procedures applicable to electronic data and suggesting changes to these policies and procedures to better protect the confidentiality and security of district data. The ISO will work with the district's technology department to advocate for resources and implement best practices to secure the district's data.

Janay Heiney - Bookkeeper is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

4. **Data Managers**

All district administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the district's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the district and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing district policies and procedures regarding data management.

5. **Confidential and Critical Information**

The district will collect, create or store confidential information only when the superintendent or designee determines it is necessary. The district will provide access to confidential information to appropriately trained district employees and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the district.

District employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the district's superintendent, ISO or designee is authorized to secure resources to assist the district in promptly and appropriately addressing a security breach.

Likewise, the district will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed, or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

All district staff, volunteers, contractors, and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using

confidential and critical information will strictly observe protections put into place by the district including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

6. **Using Online Services and Applications**

District staff members are encouraged to research and utilize online services or applications to engage students and further the district's education mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or employees, the ISO or designee must approve the use of the service or application and verify that it meets the requirements of the law and Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

7. **Training**

The ISO will provide appropriate training to employees who have access to confidential or critical information to prevent unauthorized disclosures or breaches in security. In accordance with law, all school employees will receive annual training in the confidentiality of student records.

8. **Data Retention and Deletion**

The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on district technology resources. The retention schedule must comply with the Public School District Records Retention Manual as well as the General Records Retention Manual published by the Missouri Secretary of State.

9. **Litigation Hold**

In the case of pending or threatened litigation, the district's attorney will issue a litigation hold directive to the superintendent or designee. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by the district's attorney. E-mail and other technology accounts of separated employees that have been placed on a litigation hold will be maintained by the district's information technology department until the hold is released. No employee who has been notified of a litigation hold may alter or delete any electronic record that falls within the scope of the hold.

Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

10. Consequences

Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the district. The district will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the district reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

The district may suspend all access to data or use of district technology resources pending an investigation. Violations may result in temporary, long-term, or permanent suspension of user privileges. The district will cooperate with law enforcement in investigating any unlawful actions. The superintendent or designee has the authority to sign any criminal complaint on behalf of the district.

Any attempted violation of district policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

D. Data Governance and Security – Incident and Data Breach Response Plan (EHBC-AP1)

The goal of the district is to eliminate security incidents and avoid any breach of district data. For that reason, all district employees and agents are required to immediately report to the information security officer (ISO) or designee when they know or suspect that a security incident or data breach has occurred. The superintendent, the ISO and their designees are authorized to contact the district's attorney or other necessary resources to quickly and appropriately address a security incident.

1. Definitions

Data Breach, Breach of Security or Breach – A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information. A breach includes, but is not limited to, incidents in which confidential or critical data has potentially been accessed without authorization or stolen; confidential or critical data has been compromised; or a network hack or intrusion has occurred. Good-faith acquisition of personal information by a district employee or agent for a legitimate district purpose is not a breach of security provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

Personal Information – An individual's first and last name or first initial and last name in combination with any one or more of the following:

a) Social Security number.
b) Missouri Student Identification System (MOSIS) number, driver's license number or other unique identification number created or collected by the district or any other government body.
c) Financial account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.
d) Unique electronic identifier or routing code, in combination with any required security code, access code or password that would permit access to an individual's financial account.
e) Any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional.

f) An individual's health insurance policy number, subscriber identification number or any unique identifier used by a health insurer to identify an individual.

Personal information does not include information that is encrypted, redacted or altered in such a manner that the name or data elements are unreadable or unusable. It also does not include information that is lawfully obtained from publicly available sources or from government records made available to the general public.

Security Incident – An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

Incident Response

Once notified of an event, the ISO or designee will identify and remedy the weakness that allowed the security incident to occur, repair any damage that has been done, minimize risk associated with the event, and determine who caused the incident. If the incident was intentional or occurred because a user violated district policies, procedures or training, the individual will be referred to the superintendent or designee for discipline and/or other consequences.

2. Data Breach

The district's primary goal when a data breach occurs is to recover as much data as possible, provide appropriate notifications of the data breach and prevent further disclosure and harm to district students, employees and business operations.

The ISO or designee will investigate the incident immediately and make a determination as to whether a breach did occur. If a breach did occur, the following steps will be taken as quickly as possible:

a) The superintendent and other appropriate administrative staff will be notified immediately. The superintendent or designee will contact the district's legal counsel, law enforcement and the district's insurance carrier when appropriate.
b) The ISO will determine the status of the breach and will take all appropriate measures to prevent additional loss of data and future breaches.

c) If possible, the ISO will preserve any and all evidence of the breach for future investigation, prosecution, insurance claims and other legal action.
d) The ISO will determine the scope of the breach and will work with law enforcement (when appropriate), the superintendent and the district's legal counsel to determine whether district staff, impacted parents/guardians and students, or the public need to be notified and whether additional government agencies need to be involved.
e) Once the district's data has been secured, the ISO, the superintendent and other relevant staff will meet to evaluate the incident, determine the probable causes of the incident and determine what action should be taken to prevent future incidents.

3. Notice of Breach of Personal Information

Breaches of confidential personal information are particularly problematic, and the district will take additional steps to prevent theft or fraud. The superintendent and the ISO will ensure that victims of security breaches are appropriately notified as required by law.

If the superintendent or designee, after an appropriate investigation or consultation with the relevant federal, state or local agencies responsible for law enforcement, determines that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and will be maintained for five years. If the superintendent or designee determines that identity theft is reasonably likely, the district will notify, without unreasonable delay, any person whose information may have been accessed.

This notice may be delayed if a law enforcement agency informs the superintendent or designee that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request by law enforcement is made in writing or the superintendent or designee documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. Once the law enforcement agency communicates that notice may be provided, the notice will be provided without unreasonable delay.

If the district must provide notice to more than 1,000 individuals, the district will also notify the Attorney General's Office and all consumer

reporting agencies that compile and maintain files on consumers on a nationwide basis. The district will report to these entities the timing, distribution and content of the notice sent to the persons whose information may have been compromised.

4. **Notice Content**

The notice provided to persons whose information was breached shall minimally include:

a) A description of the incident in general terms.
b) A description of the type of personal information that was obtained as a result of the breach of security.
c) A telephone number that affected consumers may call for further information and assistance, if one exists.
d) Contact information for consumer reporting agencies as defined by law.
e) Advice that directs affected consumers to remain vigilant by reviewing account statements and monitoring credit reports.
f) Information about how to obtain a free credit report.

The notice may be made in writing or by e-mail if the person has agreed to receive communications from the district electronically in accordance with federal law. Telephone notice may be used if contact is made directly with the affected person.

Substitute notice may be used if the cost of providing notice would exceed $100,000 or if the district needs to notify more than 150,000 individuals. The district may also use substitute notice for individuals the district is unable to identify or for whom the district does not have sufficient contact information, but the district will use the regular notice for all other affected individuals.

Substitute notice shall include:

a) E-mail notice when the district has an e-mail address.
b) Conspicuous posting of the notice or a link to the notice on the district's website.
c) Notification to major statewide media.

E. Data Governance and Security – Data Management (EHBC-AP2)

The effective education of students and management of district personnel often require the district to collect information, some of which is considered confidential by law and district policy. In addition, the district maintains information that is critical to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Because it is important that the district, district employees and all users of district data are good stewards of this information, the district has created a program to ensure that all data, including confidential and critical information, is accessed and maintained appropriately.

1. Definitions

Confidential Data/Information – Information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information (PII) regarding students and employees.

Critical Data/Information – Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential.

2. Data Inventory and Classification

The information security officer (ISO) or designee will identify all systems containing district data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, e-mail systems, instructional software applications and others. The ISO or designee will identify the data files and data elements maintained in those files within the systems and identify confidential and critical information the district possesses or collects. All district employees are directed to assist the ISO or designee in identifying confidential and critical information and explain the sources of the data and the purposes for which the data is collected and used so that file classification is accurate.

Once the data files and data elements are identified, the ISO will classify the data as confidential or critical so that those files and the information they contain can be more closely monitored. Additional classifications may be added as necessary to assist in monitoring and data governance.

Once the data is classified, the ISO or designee will create a data inventory. The data inventory will include documentation of the location

of the files, the persons assigned to manage the files, and the employees or employee categories that have access to the files. The ISO will maintain the district's data inventory in both electronic and printed form and will update it annually.

3. Creating, Accessing and Using Data

Data will be collected, maintained and used by the district only when it is needed for the district to fulfill its education mission. Authorized district employees, volunteers, district agents and vendors may create, access and use district data when necessary to provide services to the district, but they must do so in a manner that ensures that the data is accurate, complete, timely and relevant. Authorized users must obtain permission from the district to use the data for other purposes, including personal purposes.

The security of confidential information, including confidential PII and critical information, is particularly important, and authorized users of this information may access the information only when necessary to perform their duties for the district. The district's security administrator will work with the superintendent and relevant supervisors to determine which persons are authorized to create, access and use confidential or critical information. Confidential and critical information can only be used in accordance with state and federal confidentiality laws and district policies and procedures regarding confidential information. Confidentiality laws include, but are not limited to, the Family Educational Rights and Privacy Act, the Protection of Pupil Rights Amendment, the Children's Online Privacy Protection Act, the Missouri Safe Schools Act, the Missouri Sunshine Law, and various criminal statutes. Relevant policies include, but are not limited to, the policies cross-referenced in policy EHBC.

Unless permission has been granted by the security administrator, no employee, vendor or other person may remove confidential or critical data from the district's premises or the district's network, remove a device containing confidential or critical data from the district's premises, or modify or copy confidential or critical data for use outside the district. If permission is given, the data may be accessed only on a district-provided device with appropriate security controls or through a secure virtual private network (VPN). When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied or

otherwise used in a manner that would compromise the security and confidentiality of the information.

4. **Maintaining Data**

Confidential and critical information will be saved and maintained in a secure manner using encryption or other password-protected security measures. Likewise, when data is transmitted, the district will use encryption or password-protected security measures.

5. **Dissemination and Disclosure of Data**

District data is collected and maintained to further the district's education mission. A district employee or other authorized user of the district's data may use and disseminate it in furtherance of his or her job duties with the district as long as confidentiality laws and district policies and procedures are followed. Authorized users must obtain permission from the district before disseminating data for other purposes, including personal purposes. All requests for district information by the media or members of the public under the Missouri Sunshine Law will be directed to the district's custodian of records, who will respond to those requests as required by law.

Authorized users of confidential information are prohibited from disseminating the information to unauthorized persons unless the user is required by law to share the information, is authorized in Board policy or procedure to do so or is directed by his or her supervisor to do so. Confidential and critical information that is disseminated electronically must be encrypted or password protected.

In some circumstances confidential information can be shared when it has been redacted or altered so that the information is not personally identifiable and is no longer considered harmful or an invasion of privacy. An authorized user has the responsibility of verifying with his or her supervisor or the district security administrator whether the information has been sufficiently altered or redacted prior to releasing the information.

Authorized users of critical information that is not confidential may disseminate the information in accordance with their duties or when required by law, but such dissemination must be done in a manner that protects the security and integrity of the information.

Retaining, Archiving and Destroying Data

6. **Retaining and Archiving Information**

The ISO, in consultation with the district's custodian of records, data managers and other qualified staff, shall establish a retention schedule for the regular archiving and deletion of data stored on district technology resources. The retention schedule must comply with the Public-School Records Retention Schedule and the General Records Retention Schedule published by the Missouri Secretary of State.

Permanent records may be maintained by storing such records in a digital or electronic format for the manufacturer-suggested or recommended period of time. If the ISO chooses to store permanent records electronically, the district will follow all guidelines, suggestions or recommendations set forth by the manufacturer.

7. **Litigation Hold**

If the district's attorney notifies the district that, due to litigation, certain records cannot be deleted, the directive will be communicated to the ISO and the relevant staff. Once notified, no employee, volunteer, agent or vendor is allowed to alter, delete or destroy any information that might be relevant to the pending litigation, regardless of how the information is maintained.

8. **Destruction of Information**

Once data is no longer needed, the ISO will work with the data managers to ensure that it is appropriately destroyed. Special care will be taken to ensure that confidential information is destroyed appropriately and in accordance with law. Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record unretrievable. The ISO is authorized to use the district's procurement process to contract with an independent contractor with expertise in the area for records disposal.

9. **Removal of Information from Devices**

Before a computer, tablet or other device is sold as surplus property, transferred to another person or used for a different purpose than originally intended, the ISO or designee will remove all confidential and critical information from the device.

10. **Monitoring Release of Confidential Information**

The ISO will work with data managers to monitor how confidential data is used and released and to verify that district policies and procedures governing access to the information are being followed.

11. Monitoring Service Providers

The district uses attorneys and other specialized service providers as independent contractors. When necessary, these service providers are given access to confidential and critical information electronically or in other forms. The ISO will periodically audit the agreements and working relationships with these contractors to determine whether access to confidential or critical information is necessary and ensure that the data is appropriately used and protected.

12. Monitoring Vendors of Electronic Services

District employees are prohibited from installing software or using any online system that stores, collects or shares confidential or critical data until the ISO approves the vendor and the software or service used. This applies even if the software or system is free. All users must comply with copyright and licensing requirements and are prohibited from copying or using district licenses at home or for personal use unless authorized by the ISO.

The ISO will establish a process for ensuring that software and systems the district purchases or uses comply with the district's data security principles. The ISO will maintain a copy of all contracts with vendors that impact the district's data or data security. All contracts with vendors will conform with the requirements of state and federal law and will require the vendor to appropriately secure district data.

Before authorizing the use of a vendor, software or service in which confidential or critical data will be stored, collected or shared, the ISO will ensure that the vendor, software or service will adequately protect the district's data and act in the district's interests. All vendors, software or services used must conform to the following unless otherwise authorized by the superintendent or Board:

a) The district continues to own the data shared with the vendor, and all data must be available to the district upon request.
b) The vendor's access to and use of district data is limited; the data cannot be used for marketing, advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district.
c) If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
d) District data will be stored only on servers in the United States.

e) District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
f) The vendor, software or service will detail how and when district data will be destroyed.
g) In the event of a data breach, the vendor will immediately notify the ISO. Further, the vendor will assume liability for any breach of data when such data is being collected or manipulated by the vendor or is in the possession or control of the vendor.
h) There must be consequences and penalties if the vendor or online system discloses or uses district data inappropriately, without authorization or in violation of the law.
i) The district is entitled to monitor and audit the vendor or online system to ensure compliance with the agreement.
j) Products and services provided by the vendor will be provided in a manner that accommodates persons with disabilities in accordance with the requirements of the Americans with Disabilities Act and other applicable state and federal laws.

The ISO or designee will periodically review the overall performance of vendors and determine whether the:

a) Vendor is in compliance with the contract.
b) District is receiving value.
c) District's data is maintained securely.
d) Vendor has addressed any concerns raised by the district.

13. Free Electronic Services

District employees are prohibited from sharing confidential information or requiring students or other employees to share their confidential information using free online services unless the ISO has verified that the service complies with the same expectations as those listed in this procedure for paid vendor services and that the service is operated in compliance with confidentiality laws and district policies.

14. Security Awareness Program

The ISO will work with data managers to develop and implement a security and privacy awareness program for all staff who have access to the district's confidential and critical data as part of their employment. The goals of the security awareness program are to:

a) Enhance district data security by improving awareness of the need to protect system resources.

b) Develop skills and knowledge so computer users can perform their jobs more securely.
c) Build in-depth knowledge, as needed, to design, implement or operate security programs.

The program will include training on a recurring basis, communication of privacy policies, and communication of the process for reporting privacy incidents and submitting complaints.

15. Electronic Access Banners

The security and privacy awareness program will include the use of electronic messages (electronic access banners) that appear when users access district data electronically and that regularly remind users of privacy and security information, including the following notices:

a) The user is accessing a district-provided information system.
b) Usage of the system may be monitored, recorded and subject to auditing.
c) Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties.
d) Use of the system constitutes agreement with the terms listed on the banner.

F. Data Governance and Security – Account Management (EHBC-AP3)

The information security officer (ISO) will implement the following procedures for granting, modifying, and terminating access to the district's network or confidential or critical district information. Such access is a privilege, not a right, and access may be terminated by the ISO at any time for any legal reason.

1. Granting User Access

User access will be based solely on whether the individual needs access to the information and will not be based on the person's position in the district or title. For example, even the superintendent will not necessarily have access to all information in the district at all times if such access is not necessary to perform his or her job responsibilities.

The human resources department will notify the ISO when an employee is assigned to a new position or given additional duties and will work with the ISO or designee to determine the appropriate level of employee access to confidential or critical information.

Departments that engage independent contractors, vendors or volunteers who need to access the district's network or secure files must contact the ISO. Contractors, vendors and volunteers will be granted access to the district's network or secure files only after agreeing in writing to maintain the confidentiality and security of the information and follow the district's policies, procedures and security rules. Access will be limited to the information the contractor, vendor or volunteer needs and will be terminated after a specific period of time.

Students may be granted access to limited portions of the district's network. The ISO will work with building principals to determine the extent of the access.

2. Requests for Greater Access

A user who desires greater access than has been granted must contact the ISO to request a change of credentials. Access will not be granted unless the user demonstrates a need to know the information, as determined by the ISO in consultation with the employee's supervisor.

The ISO will keep records of level of access by role or position and records of any exceptions made when additional access is needed by a user. These records will be updated regularly.

3. Alternate or Emergency Access

District employees who work with critical business functions or confidential information are encouraged to designate one or more

alternate employees who will perform those functions in their absence or in an emergency situation. The ISO will document these designations so that the alternate is given the necessary access immediately upon notification that access is needed.

4. **User Identification and Password Requirements**

The district will require all users to have a unique user identification and a secure password before accessing confidential or sensitive district information. The district will require strong password controls of appropriate length and complexity and will prevent users from relying on previously used passwords. The district will utilize the district's network management system to enforce those requirements.

Passwords necessary to access district confidential or critical data will be changed at least every 90 days. Passwords to access other district data will be changed at least every six months. Users are prohibited from sharing their user identifications and passwords with others or using another person's user identification and password.

5. **Resetting Lost or Compromised Passwords**

Users and employees who have reason to believe a password is lost or compromised must notify the ISO or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

6. **Terminating User Access**

When short-term users (such as substitute employees, vendors and independent contractors) are provided access to the district's network, the ISO or designee will document a date when access will end, if possible, or document a date when the ISO or designee will inquire about continued access.

The human resources department will notify the ISO or designee when an employee resigns or is terminated, put on administrative leave or deemed to be a security risk. Once notified, the ISO or designee will terminate the employee's access on the appropriate effective date.

Students will generally be given continued, limited access to the district network until they graduate from the district. District principals or their designees will notify the ISO or designee when a student withdraws, transfers, graduates, is put on a long-term suspension, has lost technology privileges, or is deemed to be a security risk. The ISO or designee will terminate the student's access on the appropriate effective date.

Access to is appropriate given the user's position. Based on the review, access rights may be added, changed or removed.

7. **Monitoring Inactive Accounts**

The ISO or designee will routinely review account access logs for unusual activity or inactivity. If an employee has been given access to an area but has not accessed information from that area for more than a year, the ISO will consult with the employee's supervisor to determine whether access is still needed.

8. **Concurrent Access**

The ISO or designee will ensure that the district uses software controls, when available, to restrict concurrent access to district systems so that a single user can access the district's information system at only one location at any given time.

G. Data Governance and Security – Security Controls (EHBC-AP4)

1. Logical Security Controls

The district will use logical security controls, such as user identification and password access, user authentication, access rights and authority-level protocols, to maintain the security of the district's confidential and critical information. The district will use defenses to protect against viruses, malware, spyware, phishing and spam. Users are prohibited from turning off or disabling district protection systems.

2. Physical Security Controls

The district will use physical security controls to maintain the security of the district's confidential and critical information. The information security officer (ISO) will create and maintain physical security controls that protect district servers, network routers and essential network equipment from unauthorized access or theft and damage from fire, water, extreme temperature changes and power outages. The ISO will create locked, physical barriers to this equipment, such as locked doors or cages.

The ISO will determine who will be allowed access to essential district equipment. Those with authorized access will be provided keys or access codes to the physical barriers. The keys and access codes cannot be shared without the ISO's permission, and the ISO must be notified immediately if the keys or access codes have been compromised. The district will record who accesses essential district equipment, electronically or otherwise, using appropriate security devices, such as keys, electronic key logs, security cameras or other appropriate measures.

The ISO may temporarily grant access to a vendor or other person when determined necessary. The name of the person, the reason for the access and the date and time of the access will be documented, and the ISO will determine whether the person needs to be accompanied by district staff before access is granted.

Physical records that include critical and confidential information will be stored in locked cabinets or in rooms with limited access. The superintendent or designee will determine who will have access to these records and will distribute keys or access codes.

3. Security Logs

The ISO will identify the types of security events the district will log and monitor and will ensure that the district's network management

system's logging settings are appropriately used. The district's incident logs will include appropriate information so that the district can monitor significant system events. At a minimum, the district will log access to sensitive or critical system resources or information, data breaches and compromised account credentials.

4. **Security Audit**

The ISO or designee will regularly audit the district's security controls and make adjustments as necessary. All audits will be documented.

Business Continuity and Data Recovery Plan

5. **Backing Up Data**

The ISO will create a process by which critical district data will be backed up and stored in more than one location, and one such location must be off district property or in a different building. The ISO will ensure that the backup data is tested and validated to ensure that the backup is occurring, and information can be restored. The ISO has identified the following information as critical:

- Domain Controller
  - Incremental Backup - Daily
  - Cloud based Backup using Asigra on a laptop in server room (MoreNet can assist with restoration)
  - Local Backup in Shared folder on SV-Data
- SV-DATA
  - Local Backup on External HD connected to Server.
    - Incremental backup Daily
  - Three total copies
    - One Connected to Server
    - One Full Backup – Monthly in cabinet in Superintendent Office
    - One Full Backup – Annual in safe at Tech Directors House

6. **Alternative Data-Processing Site**

Some events, such as a tornado or flood, prevent the district from using its own equipment to restore or process backed-up data. For that reason, the district has designated the Elementary FEMA Building as its alternative data-processing site.

The ISO and designated employees will be trained in how to restore data using the alternative data processing site.

7. **Restoring Critical Systems and Data**

If an event occurs that prevents district staff from accessing critical information, the ISO or designee will access and restore the backup data. Because it will take time to restore massive amounts of data, unless the ISO determines otherwise, data will be restored in the following order:

1) Domain Controller
2) SV-DATA (Required files first)
3) SV-DATA (Teacher Files)

8. **Testing Continuity Plan**

The ISO and designated staff will routinely test the district's continuity plans to ensure that they are effective, to identify weaknesses in the plan, and to ensure that designated staff have received adequate training.

X. Technology Current State

This is the state of the Summersville R-II School District technology as of February 2023. We have come a long way in the past year and a half. Replacing all but two Windows 7 computers with Windows 10. Removing all of the expired Chromebooks from the system. Updating the screens in the classrooms from Smartboards to Promethean/ViewSonic Boards at the Elementary and Vivi Boards at the High School. We added monitoring software for the teachers to use when kids are working on Chromebooks. We changed the policy on how Chromebooks are assigned, stored, and charged putting the responsibility on the kids rather than the teachers.

We still have a long way to go, we are waiting for network equipment to come to hopefully resolve our biggest issue as of now. Our server is five years old and has shown some potential issue cropping up in the last few weeks. One issue was one of the power supplies overheated and tripped. Removing it from the server letting it cool down and putting it back in and it came back up with no issues. This issue could have been related to our Firewall power supply giving out around the same time. This caused our network to be disabled for a full day, we were able to get it back to full function by turning an old desktop computer into a firewall. Once the part came in for the actual firewall the backup device was put on a shelf and preserved as a backup plan.

The following is a full list of equipment and software owned and managed by Summersville R-II School District:

A. Hardware

1) Server
    a. HP Proliant Server
    b. Installed in 2017
    c. Two VM's running SV-PDC and SV-DATA
    d. Roughly 1.6TB of space with PDC containing 100 GB and SV-DATA containing 1TB for shared space and 100GB for Operating
    e. Managed with
2) Meraki Network
    a. 15 Switches
    b. 44 Access Points
    c. Installed in 2015-2016
    d. Increasing number of issues limping by while waiting for the remainder of equipment to arrive that was ordered in June 2022
3) Computers
    a. Desktops
        i. 50 Devices
            1. Business Room, AG, Library, Secretaries, Teachers Workroom

   b. Laptops
      i. 50 Teacher Laptops
4) Chromebooks
   a. 500 Devices
5) Grand Stream Phone System
   a. 2 Servers
   b. 57 Phones
6) Fortinet Firewall
7) Classroom Screens
   a. 11 Promethean Boards
   b. 11 ViewSonic Boards
   c. 17 Vivi Devices
   d. 3 Epson Projectors
8) SmartBus
9) Apple iPads

B. Software

1) Google Console
2) Email
3) Chromebook Control
4) Edmentum
5) Securly
   a. Classroom Monitoring
   b. Filtering
   c. Aware
6) Tyler SIS (Going to Infinite Campus in June)
7) Office 365
8) Saavas
9) Renaissance
10) Study Island
11) Akamai
12) I-Ready
13) School Website (Wordpress)

C. Physical Security

1) Physical Keys
2) 12 Year old analog camera system

XI. Future Plans

Technology planning is tough. The industry is so fluid and fast paced that priorities change almost daily depending on what is going in that particular moment. Current focus is heavy on the network infrastructure, physical security, cybersecurity, server refresh, and redundancies.

A. 1 Year Plan

No Particular Order

1) Cybersecurity
    a. Training Programs
    b. Phishing Exercises
    c. System Hardening via Group Policy, Filters, Firewall
2) Server
    a. Server Refresh using old server as redundancy
3) Firewall Redundancy
4) Upgrade Physical Security

B. 2 Year Plan

1) Begin 5-year hardware rotation on
    a. 20 Computers
    b. 100 Chromebooks
    c. 1 Piece of major hardware
        i. Network
        ii. Server
        iii. Firewall
        iv. Phones?
        v. Screens

C. 5 Year Plan

Continue to evaluate systems and change priorities as needed. 5 year plan is to refresh equipment on a schedule. The schedule will be released upcoming.