MEMORANDUM

TO: TEENA JONES

FROM: KIM ARRINGTON, TECHNOLOGY COORDINATOR KA

DATE: FEBRUARY 2, 2015

SUBJECT: DATA GOVERNANCE POLICY

I would like to request Board approval of the Chilton County Board of Education Data Governance and Use Policy at the February Board meeting. See attached copy of the policy. I will also email a copy of the policy so that you can forward it to each Board member.

APPROVED
CHILTON COUNTY BOARD OF EDUCATION
DATE 2-17-15
SUPERINTENDENT

Chilton County Board of Education
Data Governance and Use Policy

I. POLICY

A. It is the policy of Chilton County Board of Education that information, as defined hereinafter, in all its forms—written, recorded electronically or printed—shall be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection shall include an appropriate level of security over the equipment and software used to process, store, and transmit that information. Protecting our students' and staff's privacy is an important priority. The Data Governance document includes information regarding the Data Governance Committee, the Data Governance and Use Policy, Appendices, and Supplemental Resources.

B. The data governance policies and procedures are documented and reviewed annually by the data governance committee.

C. The Chilton County Board of Education Data Governance committee consists of the Superintendent, Assistant Superintendent, Technology Coordinator, Network/IT Specialist, Technology Specialist, Chief Financial Officer, and a Principal from one school within the District.

D. The Data Governance committee will meet annually. Additional meetings will be called as needed. Training on the Data Governance Policy will be conducted for all personnel annually and training will be documented. The Data Governance and Use Policy will be posted on the district website.

II. SCOPE

The policy, standards, processes, and procedures apply to all students and employees of the district, contractual third parties and agents of the district who have access to district information systems or information.

This policy applies to all forms of information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or radio
- Hard copy data printed or written on paper
- Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.
- Stored and processed by servers, PC's, laptops, tablets, mobile devices, etc.
- Stored on any type of removable media or cloud based services

REGULATORY COMPLIANCE

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems. Chilton County Board of Education complies with all applicable regulatory acts including but not limited to the following:

CIPA: The Children's Internet Protection Act was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. See http://www.fcc.gov/guides/childrens-internet-protection-act for details.

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information; see www.coppa.org for details.

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data. See http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html for details.

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well. See http://www.hhs.gov/ocr/privacy/hipaa/understanding for details.

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. See www.pcisecuritystandards.org for details.

III. RISK MANAGEMENT

A. A thorough analysis of all Chilton County Board of Education information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity, which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.
From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined at the entity level.

B. The Superintendent or designee will administer periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

IV. INFORMATION SECURITY DEFINITIONS

Affiliated Covered Entities: Legally separate, but affiliated, covered entities which choose to designate themselves as a single covered entity for purposes of HIPAA.

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

HIPAA: The Health Insurance Portability and Accountability Act, a federal law passed in 1996 that affects the healthcare and insurance industries. A key goal of the HIPAA regulations is to protect the privacy and confidentiality of protected health information by setting and enforcing standards.

Integrity: Data or information has not been altered or destroyed in an unauthorized manner.

Involved Persons: Every worker at Chilton County Board of Education -- no matter what their status. This includes nurses, residents, students, employees, contractors, consultants, temporaries, volunteers, substitutes, student teachers, interns, etc.

Involved Systems: All computer equipment and network systems that are operated within the Chilton County Board of Education environment. This includes all platforms (operating systems), all computer sizes (personal digital assistants, desktops, mainframes, etc.), and all applications and data (whether developed in-house or licensed from third parties) contained on those systems.

Personally Identifiable Information (PII): PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

V. INFORMATION SECURITY RESPONSIBILITIES

A. **Data Governance Officer:** The Data Governance Officer (DGO) for each district is responsible for working with user management, owners, custodians, and users to develop and implement prudent security policies, procedures, and controls, subject to the approval of Chilton County Board of Education. Specific responsibilities include:

1. Ensuring security policies, procedures, and standards are in place and adhered to by entity.
2. Providing basic security support for all systems and users.
3. Advising owners in the identification and classification of computer resources. See Section VI Information Classification.
4. Advising systems development and application owners in the implementation of security controls for information on systems, from the point of system design, through testing and production implementation.
5. Educating custodian and user management with comprehensive information about security controls affecting system users and application systems.
6. Providing on-going employee security education.
7. Performing security audits.
8. Reporting regularly to the Chilton County Board of Education Data Governance Committee on entity's status with regard to information security.

B. **Information Owner:** The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the Chilton County Board of Education Information Owner Delegation Form. The owner of information has the responsibility for:

1. Knowing the information for which she/he is responsible.
2. Determining a data retention period for the information, relying on advice from the Legal Department.
3. Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used or created within the unit.
4. Authorizing access and assigning custodianship.
5. Specifying controls and communicating the control requirements to the custodian and users of the information.
6. Reporting promptly to the DGO the loss or misuse of Chilton County Board of Education information.
7. Initiating corrective actions when problems are identified.
8. Promoting employee education and awareness by utilizing programs approved by the DGO, where appropriate.
9. Following existing approval processes within the respective organizational unit for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.

C. **Custodian:** The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner. Responsibilities may include:

1. Providing and/or recommending physical safeguards.
2. Administering access to information.
3. Releasing information as authorized by the Information Owner and/or the Information Privacy/ Security Officer for use and disclosure using procedures that protect the privacy of the information.
4. Evaluating the cost effectiveness of controls.
5. Maintaining information security policies, procedures and standards as appropriate and in consultation with the DGO.
6. Promoting employee education and awareness by utilizing programs approved by the DGO, where appropriate.
7. Reporting promptly to the DGO the loss or misuse of Chilton County Board of Education information.
8. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

D. **User Management:** Chilton County Board of Education management who supervise users as defined below. User management is responsible for overseeing their employees' use of information, including:

1. Reviewing and approving all requests for their employees access authorizations.
2. Initiating security change requests to keep employees' security record current with their positions and job functions.

3. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.
4. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.
5. Providing employees with the opportunity for training needed to properly use the computer systems.
6. Reporting promptly to the DGO the loss or misuse of Chilton County Board of Education information.
7. Initiating corrective actions when problems are identified.
8. Following existing approval processes within their respective organization for the selection, budgeting, purchase, and implementation of any computer system/software to manage information.
9. Subs and Temporary Employees are not granted network access. Subs hired as long-term substitutes, per Board approval, will be granted network access.

E. **User:** The user is any person who has been authorized to read, enter, or update information. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.
2. Comply with Information Security Policies and Standards and with all controls established by the owner and custodian.
3. Keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential.
4. Report promptly to the DGO the loss or misuse of Chilton County Board of Education information.
5. Initiate corrective actions when problems are identified.
6. All new teachers and staff will complete training on all District technology policies.

VI. INFORMATION CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

A. **Personally Identifiable Information (PII)**

1. PII is any information about an individual maintained by an agency:
   a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number,

date and place of birth, mother's maiden name, or biometric records.

b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

2. Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious damage to Chilton County Board of Education.

B. **Confidential Information**

1. Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

2. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for Chilton County Board of Education, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

C. **Internal Information**

1. Internal Information is intended for unrestricted use within Chilton County Board of Education, and in some cases within affiliated organizations such as Chilton County Board of Education business partners. This type of information is already widely distributed within Chilton County Board of Education, or it could be so distributed within the organization without advance permission from the information owner.
Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

2. Any information not explicitly classified as PII, Confidential or Public will, by default, be classified as Internal Information.

3. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

D. **Public Information**

1. Public Information has been specifically approved for public release by a designated authority within each entity of Chilton County Board of Education. Examples of Public Information may include marketing brochures and material posted to Chilton County Board of Education's web pages.

2. This information may be disclosed outside of Chilton County Board of Education.

VII. COMPUTER AND INFORMATION CONTROL

All involved systems and information are assets of Chilton County Board of Education and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Ownership of Software:** All computer software developed by Chilton County Board of Education employees or contract personnel on behalf of Chilton County Board of Education or licensed for Chilton County Board of Education use is the property of Chilton County Board of Education and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. **Installed Software:** All software packages that reside on computers and networks within Chilton County Board of Education must comply with applicable licensing agreements and restrictions and must comply with Chilton County Board of Education acquisition of software policies.

C. **Virus Protection:** Virus checking systems approved by the Data Governance Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus-checking systems.

D. **Access Controls:** Physical and electronic access to information systems that contain PII, Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the data governance committee and approved by Chilton County Board of Education. In particular, the data governance committee shall document roles and rights to the student information system and other like systems. Mechanisms to control access to PII, Confidential and Internal information include (but are not limited to) the following methods:

1. **Authorization:** Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the assistance of the DGO. Any of the following methods are acceptable for providing access under this policy:

a. *Context-based access:* Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.

b. *Role-based access:* An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

c. *User-based access:* A security mechanism used to grant users of a system access based upon the identity of the user.

2. **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PII, Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

   a. At least one of the following authentication methods must be implemented:
      1. Strictly controlled passwords (Section VIII – Password Control Standards),
      2. Biometric identification, and/or
      3. Tokens in conjunction with a PIN.

   b. The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

   c. An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).

   d. The user must log off or secure the system when leaving it.

3. **Data Integrity:** Chilton County Board of Education must be able to provide corroboration that PII, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

   a. Transaction audit
   b. Disk redundancy (RAID)
   c. ECC (Error Correcting Memory)
   d. Checksums (file integrity)
   e. Encryption of data in storage
   f. Digital signatures

4. **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

   a. Integrity controls and
   b. Encryption, where deemed appropriate

5. **Remote Access:** Access into Chilton County Board of Education network from outside will be granted using Chilton County Board of Education approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PII, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the Chilton County Board of Education network.

6. **Physical Access:** Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.
The following physical controls must be in place:

   a. Computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
   b. File servers containing PII, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
   c. Onsite Active Directory/DHCP Servers shall be accessed by authorized personnel only.
   d. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards.
   e. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

      1. Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
      2. Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      3. Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
      4. Maintenance records – Documented policies and procedures to document repairs and modifications

to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

7. **Physical Security**: Controls are implemented to protect information system resources, the facility housing those resources, and the facilities used to support their operation. To protect against loss of control over system integrity and system availability, organizations need to address physical access controls, environmental controls, fire safety, and protect systems and data storage media from theft.

OBJECTIVE:
This policy communicates the essential aspects of physical security of computing equipment and data storage media that must be practiced by all information technology organizations to safeguard the integrity and availability of State information system resources and data.

RESPONSIBILITIES:
Agency Management, Information Technology Organization:

- Ensure computer systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Ensure laptop and portable computers are secured with an appropriate physical security device such as a lockdown cable. Computer equipment installed in public areas shall be similarly secured.
- Control access to areas containing servers, data stores, and communications equipment. Access to secured areas shall be controlled by the use of access card keys, access code keypads, or key locks with limited key distribution. A record shall be maintained of all personnel who have authorized access.
- Closely control keys (where utilized). If a key is reported as missing, change or re-key the corresponding lock(s).
- Change access codes, where utilized, immediately upon removing someone from the authorized access list.
- Maintain a log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months.

- Ensure visitors are escorted by a person with authorized access to the secured area.
- Ensure each facility containing computer and communications equipment has an appropriate fire suppression system and/or a class C fire extinguisher readily available and in working order.
- Store equipment above the floor, in racks whenever feasible, or on a raised floor to prevent damage from dampness or flooding. Use of water/moisture sensors is recommended.
- Monitor and maintain data center temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
- Store electronic media in secured and environmentally controlled areas, in fire safe containers whenever feasible. Backup/archive media shall, whenever feasible, be stored in a secure off-site storage facility.
- Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. Maintain a record of all such items entering or exiting their assigned location.
- Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

8. **Emergency Access:**

a. Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

b. Procedures must be documented to address:

1. Authorization
2. Implementation
3. Revocation

9. **Preventative Measure:**

a. Ensure only authorized personnel have access to INOW and other applications that contain personal information.

b. Do not use social security numbers on printed documents unless absolutely necessary.

c. Shred any printed documents with personal information that was printed and is no longer needed.

d. BE SURE ALL EMPLOYEES "Lock" or Log Off their workstations when away from their desks. (See instructions below).

e. Ensure your employees are not giving out phone numbers or other personal information about employees or students to anyone who is not requesting it for an official business purpose. (Do not allow employees to give out the home phone numbers of parents or employees as a courtesy to someone who asks for it.)

E. **Equipment and Media Controls:** The disposal of information must ensure the continued protection of PII, Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

1. **Information Disposal / Media Re-Use of:**
   a. Hard copy (paper and microfilm/fiche)
   b. Magnetic media (floppy disks, hard drives, zip disks, etc.)
   c. CD ROM Disks

2. **Accountability:** Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3. **Data backup and Storage:** When needed, create a retrievable, exact copy of electronic PII before movement of equipment.

4. **Disposal of Hardware:** Prior to disposal of any computer, the user will notify the Technology Department. The Tech Coordinator/Technician will remove the hard drive from the device and destroy it prior to the device being disposed of or auctioned off.

F. **Other Media Controls:**

1. PII and Confidential Information stored on external media (diskettes, CD-ROMs, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as PII or Confidential Information. Further, external media containing PII and Confidential Information must never be left unattended in unsecured areas.
2. PII and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:
   a. Power-on passwords
   b. Auto logoff or screen saver with password

c. Encryption of stored data or other acceptable safeguards approved by Data Governance Officer

Further, mobile computing devices must never be left unattended in unsecured areas.

3. If PII or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of Chilton County Board of Education Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with Chilton County Board of Education.

G. **Data Transfer/Exchange/Printing:**

1. **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass downloads of, or individual requests for, information for research or any other purposes that include PII must be in accordance with this policy and be approved by the data governance committee. All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Memorandum of Agreements (MOA) must be in place when transferring PII to external entities. See Appendix A.
2. **Other Electronic Data Transfers and Printing:** PII, Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. PII and Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible should be de-identified before use.

H. **Oral Communications:** Chilton County Board of Education staff should be aware of their surroundings when discussing PII and Confidential Information. This includes the use of cellular telephones in public areas. Chilton County Board of Education staff should not discuss PII or Confidential Information in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

I. **Audit Controls:** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PII must be implemented. Further, procedures must be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews must be documented and maintained for six (6) years.

J. **Evaluation:** Chilton County Board of Education requires that periodic technical and non-technical evaluations be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

K. **Contingency Plan:** Controls must ensure that Chilton County Board of Education can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain PII, Confidential, or Internal Information. This will include developing policies and procedures to address the following:

1. **Data Backup Plan (Appendix B):**
   a. A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.
   b. Backup data must be stored in an off-site location and protected from physical damage.
   c. Backup data must be afforded the same level of protection as the original data.

2. **Disaster Recovery Plan (Appendix C):** A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

3. **Emergency Mode Operations Plan (Appendix D):** A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

4. **Testing and Revision Procedures (Appendix E):** Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

5. **Applications and Data Criticality Analysis:** The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Compliance

A. The Data Governance and Use Policy applies to all users of Chilton County Board of Education information including: employees, staff, students, volunteers, substitutes, student teachers, interns and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable Chilton County Board of Education procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with Information Security Policies and Standards by students may constitute grounds for corrective action in accordance with Chilton County Board of Education procedures. Further, penalties associated with state and federal laws may apply.

B. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of PII or Confidential Information as specified in Confidentiality Statement.
2. Unauthorized disclosure of a sign-on code (user id) or password.
3. Attempting to obtain a sign-on code or password that belongs to another person.
4. Using or attempting to use another person's sign-on code or password.
5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
6. Installing or using unlicensed software on Chilton County Board of Education computers or technological systems.
7. The intentional unauthorized altering, destruction or disposal of Chilton County Board of Education information, data and/or systems.
8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

VIII. Password Control Standards

The Chilton County Board of Education Data Governance and Use Policy requires the use of **strictly** controlled passwords for accessing Personally Identifiable Information (PII), Confidential Information (CI) and Internal Information (II). (See VI of this policy for definition of these protected classes of information.)
Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards for accessing PII, CI, II:
Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person, unless the person is a designated security manager.
2. Passwords must, where possible, have a minimum length of six characters.
3. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc.). A combination of alpha and numeric characters are more difficult to guess.

Where possible, system software must enforce the following password standards:

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System software must enforce the changing of passwords and the minimum length.

4. System software must disable the user identification code when more than three consecutive invalid passwords are given within a 15 minute timeframe. Lockout time must be set at a minimum of 30 minutes.

IX. Reporting Security Breaches

All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical measures.

Chilton County School District Technological Services and Systems Memorandum of Agreement (MOA)

Appendix A

THIS MEMORANDUM OF AGREEMENT, executed and effective as of the ____ day of ______________, 20__, by and between ______________________, a corporation organized and existing under the laws of ____________________ (the "Company"), and **CHILTON COUNTY SCHOOL DISTRICT**, a public school system organized and existing under the laws of the state of Alabama (the "School Board"), recites and provides as follows.

Recitals

The Company and the School Board are parties to a certain agreement entitled "____" hereafter referred to as (the "Agreement"). In connection with the execution and delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student Personally Identifiable Information (PII) hereafter referred to as student information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

Agreement

The following provisions shall be deemed to be included in the Agreement:

Confidentiality Obligations Applicable to Certain Chilton County School District Student Records. The Company hereby agrees that it shall maintain, in strict confidence and trust, all Chilton County School District student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information will not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

The Company shall cause each officer, director, employee and other representative who shall have access to Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all Student Information. The Company shall take all reasonable steps to insure that no Student information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for Chilton County School District under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of Chilton County School District, or (c) are entitled to such student information from the Company pursuant to federal and/or Alabama law. The Company shall use student information, and shall take all reasonable steps necessary to ensure that its Authorized Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the student information as confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Alabama law; (c) maintain at all times a list of Authorized Representatives with access to student information.

Other Security Requirements. The Company shall maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e-mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify Chilton County School District of planned system changes that may impact the security of data; (g) return or destroy Chilton County School District data that exceed specified retention schedules; (h) notify Chilton County School District of any data storage outside the US; (i) in the event of system failure, enable immediate recovery of information to the previous business day. The Company should guarantee that Chilton County School District data will not be sold to, accessed by, or moved by third parties.

In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify Chilton County School District within 24 hours of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the student information compromised by the breach; (c) return compromised data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with Chilton County School District's efforts to communicate to affected parties by providing the school district with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with Chilton County School District to remediate the breach which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the disclosure; (f) cooperate with Chilton County School District by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide Chilton County School District with notice within 24 hours of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of data of any kind, failure to follow security requirements and/or failure to safeguard data. The Company's compliance with the standards of this provision is subject to verification by Chilton County School District personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and shall not be shared, sold, or moved to other companies or organizations nor should other companies or organizations be allowed access to said information.

Disposition of MBS Data Upon Termination of Agreement

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required Chilton County School District student data and/or staff data. The Company hereby acknowledges and agrees that, solely for purposes of receiving access to data and of fulfilling its obligations pursuant to this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be school officials of the School Board, and shall maintain Chilton County School District data in accordance with all federal state and local laws, rules and regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of its officers, directors, employees, agents or representatives of the obligations of the Company or its Authorized Representatives under this provision.

Certain Representations and Warranties. The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company's execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

Governing Law; Venue. Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Alabama, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Alabama.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

[COMPANY NAME]

By: ________________________________
[Name]
[Title]

CHILTON COUNTY SCHOOL DISTRICT

By: ________________________________
[Name]
Superintendent
Chilton County School District

Chilton County Board of Education
Data Backup Plan
Appendix B

I. POLICY

Electronic information must be backed up on a regular basis, for the purpose of disaster recovery and instruction resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

II. SCOPE

Data custodians are responsible for providing adequate backups to ensure the recovery of electronic information in the event of failure. These backup provisions will allow school processes, including instruction to be resumed in a reasonable amount of time with minimal loss of data. Since failures can take many forms, and may occur over time, multiple generations of backups should be maintained.

III. POLICY STATEMENT

- Backups of school records and software must be retained such that computer operating systems and applications are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data.
- Data should be backed up only if restoration is more efficient than creation in the event of failure.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, changes, and migration of applications to alternative platforms.

Chilton County Board of Education
Disaster Recovery Plan
Appendix C

I. Overview

A Disaster Recovery Plan (DRP) involves more than off-site storage or backup processing. The DRP is a written, comprehensive disaster recovery plan that addresses all the critical operations and functions of this school system. The plan includes procedures, which, if followed, will ensure the ongoing availability of critical resources and continuity of operations.

Chilton County Schools Disaster Recovery Plan (DRP) addresses a process for the recovery of both data and hardware and also addresses all critical operations should a disaster occur in the Chilton County School District. The plan is designed to minimize the impact of "down-time," and to ensure that necessary operational functions will be available for use in the least amount of time. Such operations include access to the following:

- Instructional materials
- Financial information
- Student information management systems
- Testing and accountability information
- Personnel information
- Data records

Commitment of all system personnel is necessary in order for a DRP to ensure successful recovery of data and hardware systems with the least amount of inoperable time.

II. Committee

A committee to oversee the implementation of the disaster recovery plan will be comprised of the Chilton County School District's Superintendent, Assistant Superintendent, Technology Coordinator, Technology Specialist, Network/IT Specialist, Chief Financial Officer, and a principal from one school within the District.

III. Departments—Critical needs

Critical needs are defined as the necessary procedures and equipment required to continue operations should a department, computer center, main facility or a combination of these be destroyed or become inaccessible. An evaluation for each department/school containing the following items is needed.

- Critical operations
- Current location of critical data/information
- Key personnel information
- Key systems for operation
- Needed documentation for preservation
- Vital records
- Policies and procedures
- Key data centers

IV. Data Collection

Documentation and data gathering materials for each department/school will be maintained – a copy within the school/department and a copy at the district office. Documentation and data information includes:

- Backup position listing
- Critical telephone numbers
- Communications inventory
- Distribution register
- Documentation inventory
- Equipment inventory
- Forms inventory
- Insurance policy inventory
- Main computer hardware inventory
- Master call list
- Master vendor list
- Microcomputer hardware and software inventory
- Notification checklist
- Office supply inventory
- Off-site storage location inventory
- Software and data files backup/retention schedules
- Telephone inventory
- Temporary location specifications
- Other materials and documentation

V. Backup Protection

Onsite and Offsite backups are currently being used in the Chilton County School District.

The Technology Department continues to investigate better methods for backup/protection of information. With consideration for expense, "spare" equipment is kept available.

VI. Procedure

In the event of infrastructure and/or server failure, plans for restoring computing and network facilities for Chilton County Schools are outlined below. This plan lists those measures that are in place to assist in such a recovery, as well as the actual steps taken after the disaster to begin the restoration process.

Restoration Process
District Technology Coordinator is contacted with the report of the network disaster.
District Technology Coordinator directs appropriate personnel to conduct damage assessments and construct a priority list for restoration/ recovery.
District Technology Coordinator and other appropriate personnel use the priority list to develop a strategic plan for network recovery.

District Technology Coordinator will keep the Superintendent informed of findings and plan for recovery.
Suggested prioritization of network components:

- Highest priority – network backbone (firewall, switches, wiring components, main servers that contain critical operational data)
- Medium priority – web server, web filter, email server, network print services, desktop computer of critical personnel
- Low priority – instructional computer labs, desktop computers and individual peripherals

Chilton County Board of Education
Emergency Mode Operations Plan
Appendix D

I. POLICY

This policy reflects the Chilton County Board of Education's commitment to have an emergency mode operations plan for protecting its information systems during and immediately after a crisis situation.

II. SCOPE

During an interruption of electronic services, either by forces of nature or system failures, the Chilton County Board of Education will continue school function using Emergency Mode Operations.

Chilton County Board of Education
Testing and Revision Procedures
Appendix E

I. TESTING

Testing of data backup, disaster recovery, and emergency mode operation plans should take place at least annually, with all actions documented in writing, to evaluate the effectiveness of its recovery efforts, response times, timely restoration of school operations, and safeguarding of electronic information.

II. REVISION

To be effective, Data Backup, Disaster and Recovery, and Emergency Mode Operation plans must be maintained in a ready state that accurately reflects procedures and policies. Periodic reviews of the plan must be conducted in addition to reviews whenever there are changes affecting:

- Operational Requirements
- Security requirements
- Changes of hardware, software, and other equipment
- Changes with alternate facility requirements
- Changes with team members and team members contact information

Resource 1: ALSDE State Monitoring Checklist

I. Data Governance

A. Data Governance and Use Policy

ON-SITE	YES	NO	N/A	Indicators	Notes
1. Has a data governance committee been established and roles and responsibilities at various levels specified?				• Dated minutes of meetings and agendas • Current list of roles and responsibilities	
2. Has the local school board adopted a data governance and use policy?				• Copy of the adopted data governance and use policy • Dated minutes of meetings and agenda	
3. Does the data governance policy address physical security?				• Documented physical security measures	
4. Does the data governance policy address access controls and possible sanctions?				• Current list of controls • Employee policy with possible sanctions	
5. Does the data governance policy address data quality?				• Procedures to ensure that data are accurate, complete, timely, and relevant	
6. Does the data governance policy address data exchange and reporting?				• Policies and procedures to guide decisions about data exchange and reporting • Contracts or MOAs involving data exchange	
7. Has the data governance policy been documented and communicated in an open and accessible way to all stakeholders?				• Documented methods of distribution to include who was contacted and how • Professional development for all who have access to PII	