

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, ILLINOIS, MISSOURI, NEW HAMPSHIRE, NEW YORK, OHIO,
RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME-IL-MO-NH-NY-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

Winnisquam Regional School District

and

CAP Inc. d.b.a. EPES

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Winnisquam Regional School District, located at 433 W Main St, Northfield, NH 03276 USA (the “**Local Education Agency**” or “**LEA**”) and CAP Inc. d.b.a. EPES, located at 206 N. Armstrong, Bixby, OK 74008-4309 USA (the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - ☒ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: _____ Title: _____

Address: _____

Phone: _____ Email: stacey@epes.org

The designated representative for the LEA for this DPA is:

Bailey Rigg, Director of Technology
433 W Main St, Northfield, NH 03276
6032864531 x8025
brigg@wrsdsau59.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Winnisquam Regional School District

By:  Date: 03/15/25
Bailey Rigg (Mar 15, 2025 05:47 EDT)

Printed Name: Bailey Rigg Title/Position: IT Director

CAP Inc. d.b.a. EPES

By:  Date: 1/30/2025

Printed Name: Stacey Crystal Title/Position: President

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of

all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

EPES financial and administrative software solutions designed to help schools manage budgets, accounting, and reporting efficiently.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	X

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT “G”
Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act (“LRA”), 50 ILCS 205; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: “This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed.”
2. Replace Notices with: “Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.”
3. In Article II, Section 1, add: “Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.”
4. In Article II, Section 2, replace “forty-five (45)” with “five (5)”. Add the following sentence: “In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.”

5. In Article II, Section 4, replace it with the following: “In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.”
6. In Article II, Section 5, add: “By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).”
7. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
8. In Article IV, Section 6, replace the whole section with:

The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
10. In Article IV, Section 7, add “renting,” after “using.”

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States.
12. In Article V, Section 4, add the following: “‘Security Breach’ does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.”
13. In Article V, Section 4(1) add the following:
 - vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
 - vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

 - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

 - d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.
15. Replace Article VII, Section 1 with: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.”
16. In Exhibit C, add to the definition of Student Data, the following: “Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", "student temporary record" or "student permanent record" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA."

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E:
"The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."
18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
20. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.
22. The Provider will not collect social security numbers.

EXHIBIT “G”

Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, 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
 - iv. 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
 - v. Medical information; or
 - vi. Health insurance information.

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT “G”
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"

New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **“Exhibit D”**.

11. To amend Article IV, Section 7 to add: ‘Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, “which term shall not include students.”
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department’s Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider’s expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider’s privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
 - vi. The number of records affected, if known; and
 - vii. A description of the investigation undertaken so far; and
 - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.
-

Exhibit “J”
LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at

See Attachment







EPES_Winnisquam_NH_11State_OHG_Vendor Signed

Final Audit Report

2025-03-15

Created:	2025-01-31
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAoOozqz97d7LVUj4sF-FvOvEeA1mfBX_b

"EPES_Winnisquam_NH_11State_OHG_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2025-01-31 - 7:39:40 PM GMT
-  Document emailed to brigg@wrdsau59.org for signature
2025-01-31 - 7:39:51 PM GMT
-  Email viewed by brigg@wrdsau59.org
2025-03-15 - 9:43:17 AM GMT
-  Signer brigg@wrdsau59.org entered name at signing as Bailey Rigg
2025-03-15 - 9:46:58 AM GMT
-  Document e-signed by Bailey Rigg (brigg@wrdsau59.org)
Signature Date: 2025-03-15 - 9:47:00 AM GMT - Time Source: server
-  Agreement completed.
2025-03-15 - 9:47:00 AM GMT



MBO Data, LLC dba TulsaConnect

Data Center Hosting Solutions System

SOC 1[®] Type 2 Report

May 1, 2023 to April 30, 2024

Contents

I.	Independent Service Auditor's Report.....	1
II.	MBO Data, LLC dba TulsaConnect's Management Assertion	4
III.	MBO Data, LLC dba TulsaConnect's Description of the System	6
IV.	Control Objectives, Related Controls, and Control Test Procedures and Results	13
V.	Other Information Provided by MBO Data, LLC dba TulsaConnect.....	25
	Glossary of Abbreviations and Terminologies	26



I. Independent Service Auditor's Report

To Management
MBO Data, LLC dba TulsaConnect

Scope

We have examined MBO Data, LLC dba TulsaConnect's (TulsaConnect) description of its Data Center hosting solutions system (system) throughout the period May 1, 2023 to April 30, 2024 (description), and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in TulsaConnect's assertion. The controls and control objectives included in the description are those that management of TulsaConnect believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of TulsaConnect's controls are suitably designed and operating effectively, along with related controls at TulsaConnect. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in Section V is presented by management to provide additional information and is not a part of TulsaConnect's description of its system made available to user entities during the period May 1, 2023 to April 30, 2024. Information about TulsaConnect in Section V has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description of the system, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

In Section II, TulsaConnect has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Service Organization is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period May 1, 2023 to

April 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of TulsaConnect's system and the suitability of the design and operating effectiveness of the controls involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in TulsaConnect's assertion;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by TulsaConnect in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests, are listed in Section IV.

Opinion

In our opinion, in all material respects, based on the criteria described in TulsaConnect's assertion:

- The description fairly presents the system that was designed and implemented throughout the period May 1, 2023 to April 30, 2024.
- The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period May 1, 2023 to April 30, 2024, and the subservice organizations and user entities applied the complementary controls assumed in the design of TulsaConnect's controls throughout the period May 1, 2023 to April 30, 2024.
- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period May 1, 2023 to April 30, 2024, if complementary subservice organization and user entity controls assumed in the design of TulsaConnect controls operated effectively throughout the period May 1, 2023 to April 30, 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of TulsaConnect, user entities of TulsaConnect's system during some or all of the period May 1, 2023 to April 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tulsa, Oklahoma
October 9, 2024

II. MBO Data, LLC dba TulsaConnect's Management Assertion

We, MBO Data, LLC dba TulsaConnect (TulsaConnect), have prepared the description of our Data Center hosting solutions system (system) throughout the period May 1, 2023 to April 30, 2024 (description), for user entities of the system during some or all of the period May 1, 2023 to April 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of TulsaConnect's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

- a. The description fairly presents the system made available to user entities of the system during some or all of the period May 1, 2023 to April 30, 2024, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions including, if applicable:
 - the types of services provided including, as appropriate, the classes of transactions processed;
 - the procedures, within both automated and manual systems, by which services are provided including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information presented to user entities of the system;
 - the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information presented to user entities;
 - how the system captures and addresses significant events and conditions, other than transactions;
 - the process used to prepare reports and other information for user entities;
 - services performed by a subservice organization, if any, including whether the carve-out method or inclusive method has been used in relation to them;
 - the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity and subservice organization controls assumed in the design of TulsaConnect's controls; and
 - other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control and monitoring activities that are relevant to the services provided.

- ii. includes relevant details of changes to TulsaConnect's system during the period covered by the description.
 - iii. does not omit or distort information relevant to the scope of TulsaConnect's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of TulsaConnect's system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. The controls related to the control objectives stated in the description were suitably designed and operating effectively, throughout the period May 1, 2023 to April 30, 2024, to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of TulsaConnect's controls throughout the period May 1, 2023 to April 30, 2024. The criteria we used in making this assertion were that:
 - i. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of TulsaConnect.
 - ii. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
 - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

Mike Bacher, Director of Data Center Operations

III. MBO Data, LLC dba TulsaConnect's Description of the System

OVERVIEW

MBO Data, LLC dba TulsaConnect (TulsaConnect) is a privately held provider of Data Center Hosting and associated Managed IT Services. Headquartered in Tulsa, Oklahoma, TulsaConnect operates the Data Center division of MBO, LLC (MBO).

MBO includes third-generation Oklahoma telecommunication principals. Through its subsidiaries, MBO provides voice, video, and data services on a wholesale and retail level to clients in a four-state area. MBO owns Cimarron Telephone Company and Cim-Tel Cable, Pottawatomie Telephone Company, MBO Networks, MBO Wireless, MBO Aviation, and Lakeland Properties.

The corporate sales office is located at 4500 South 129th East Avenue, Tulsa, Oklahoma, and the Data Center locations are as follows:

- **DC-3 and DC-3B:** 4500 South 129th East Avenue, Tulsa, Oklahoma 74134
- **DC-4:** 701 North Broadway Avenue, Oklahoma City, Oklahoma 73102
- **DC-5:** 110 West 7th Street, Tulsa, Oklahoma 74119

SERVICES PROVIDED

TulsaConnect provides redundant, high availability secure Data Center services for a variety of client needs. The primary offered services include Private Cloud, Shared Cloud, Colocation, and Managed IT Services (MSP).

Private Cloud

TulsaConnect supplies dedicated hardware resources (servers, firewall, and associated devices) to a single client and employs virtualization technology (such as VMware or Hyper-V) to allow for multiple VMs to be run within a cloud environment. Pricing is based on the hardware resources and managed services desired. High-availability options are available, including replication between multiple TulsaConnect Data Centers.

Shared Cloud

TulsaConnect supplies a VM instance on a shared hosting infrastructure for the client's use. Pricing is based on the physical server resources (disk, memory CPU) and services desired.

Colocation

Clients provide their own servers, network equipment, and associated devices and place them in secure racks at one of the Data Center locations. TulsaConnect supplies redundant power, network, and environmental control for a monthly fee. Pricing is based on the amount of space, power, network utilized, and other managed services required.

Managed IT Services (MSP)

TulsaConnect offers several complementary managed services along with the hosting offerings. These services include data backup, systems administration, OS install and patch updates, managed firewall and intrusion detection system, VPN and wide area network, and in-depth server monitoring.

OBJECTIVES SPECIFIED BY TULSACONNECT

The control objectives and related controls contained within Section IV are specified and maintained by TulsaConnect to define and align the operational control environment with the organizational goals and objectives established by management.

Control Objectives	
1	Controls provide reasonable assurance that management maintains segregation of duties and is responsible for oversight and consistent implementation of security practices.
2	Controls provide reasonable assurance that employees understand their responsibilities and are suitable for the roles for which they are considered.
3	Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage, and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.
4	Controls provide reasonable assurance that system availability is maintained and that systems operate in a consistent and predictable manner.
5	Controls provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.
6	Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts, and that clients understand the limits of the TulsaConnect service and their responsibility to implement network security controls.
7	Controls provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after changes.
8	Controls provide reasonable assurance that routine, client-requested, and emergency change management issues are communicated to the client.
9	Controls provide reasonable assurance that data is backed up in a secure manner for offsite retrieval and backup details are logged.

CONTROL ENVIRONMENT

The objectives of internal control as it relates to TulsaConnect's Data Center hosting solutions are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant operational needs, that assets and data are protected from unauthorized access, modification, use, or disposition, and that services are conducted in accordance with management's authorization and client instructions. Management has established and maintained controls designed to monitor compliance with TulsaConnect's policies and procedures.

GOVERNANCE AND OVERSIGHT

TulsaConnect corporate executives are responsible for business strategy, delivery of services, and the design and implementation of information security controls, as reviewed annually. Policies and procedures are documented and maintained in a centralized employee-accessible database. Continued administration of the development, implementation, and maintenance of policies and procedures is the shared responsibility of the Director of Data Center Operations and Manager of Technical Services.

Management meets periodically to review current and future business objectives, outstanding issues and to update policy, if required.

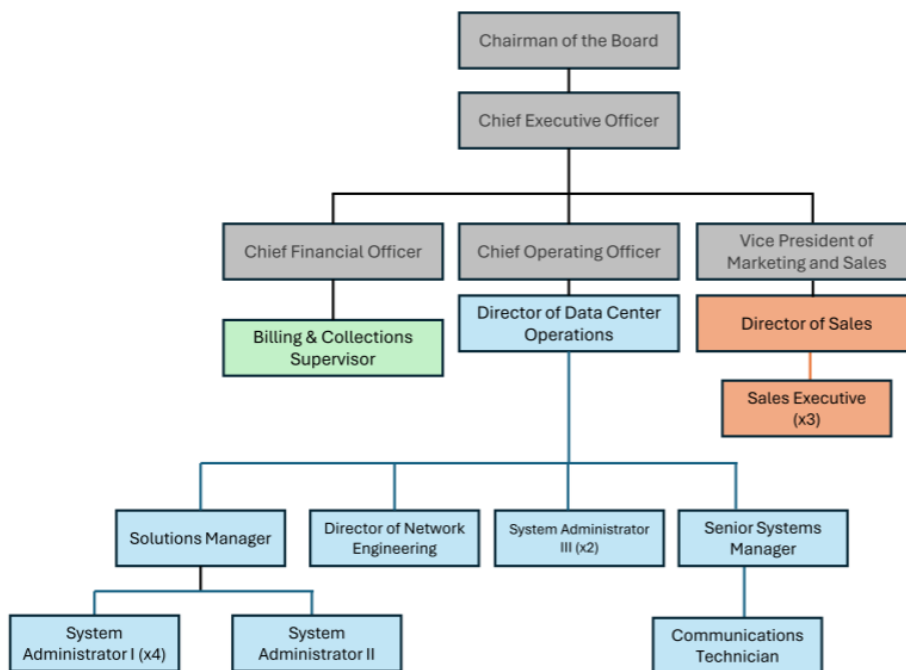
Security Management

TulsaConnect has a group of individuals who act in various capacities as it relates to security. This team consists of the Manager of Technical Services, Director of Network Engineering and Director of Data Center Operations. They are responsible for developing, maintaining, and enforcing TulsaConnect's information security policies which are reviewed annually. During annual security training and awareness programs, management ensures communication of the latest security policies, as well as written job descriptions for security management.

ORGANIZATIONAL STRUCTURE

TulsaConnect is segregated into separate functional areas to manage client information, the processing of the information, and to ensure adequate separation of duties. TulsaConnect's organizational chart reflects appropriate segregation of duties:

**TulsaConnect Organizational Chart
2023-2024**



NOTE: Titles in Gray are not TulsaConnect Employees

PERSONNEL MANAGEMENT

Employee policies and procedures are provided to employees upon hire in the Employee Handbook. New employees sign a nondisclosure agreement, as well as an acknowledgement of receipt of and compliance with the Employee Handbook. Background checks, phone screenings and/or in-person annual employee training includes HIPAA and security awareness. TulsaConnect systems administrators undergo yearly reviews to evaluate quality of work and role effectiveness.

RISK MANAGEMENT

Management updates a risk assessment of the control objectives and related controls described in this report during the annual policies and procedures review. The following types of risk are identified during TulsaConnect's risk assessment process:

- operational risks related to information systems, manual processes, and external systems;
- financial and legal risks related to market and organizational changes, regulatory costs, or other negligent action; and
- technology risks related to intrusion, fraud, system failure, and errors.

Once identified, management considers the impact potential and impact severity to establish a risk ranking for relevant threats and vulnerabilities. Impact potential is the likelihood of the vulnerability being exploited, and impact severity is how damaging an exploitation of the vulnerability would be. If a vulnerability is unlikely to be exploited and would have a minor impact, it is viewed as a relatively small risk. If a vulnerability is very likely to be exploited and would have a severe impact, it is viewed as a very significant risk. Other combinations of likelihood and severity result in establishment of a risk ranking along this continuum.

Based on the severity of risk posed by the relevant identified vulnerabilities, management ensures that the design and operation of its controls are sufficient to mitigate risks to an acceptable level.

CONTROL ACTIVITIES

TulsaConnect's control objectives and related controls are an integral part of its system description and are detailed in Section IV of this report. Management is responsible for the continued administration of the development, implementation, and maintenance of policies and procedures to direct, guide, and authorize the control activities described in the following sections.

PHYSICAL SECURITY

Physical access to the corporate offices and Data Centers is controlled by biometric access and/or locks. Biometric authentication is implemented at entrances that lead to areas where client or Data Center equipment resides. Biometric access controls recognize TulsaConnect employees via fingerprint identification. These biometric access controls record a log of individuals that entered the Data Center, including the date and time of access. Authorized users are registered in the system through a controlled, documented process.

Within the Data Centers, security fences with locked gates or locked rack cabinets protect critical infrastructure components. In shared data processing areas, client equipment is secured in locked cabinets. Client cabinets have locking front and back doors and are locked when not being accessed by a client and/or TulsaConnect staff. TulsaConnect employees are the only keyholders to the client cabinets. In addition, clients are escorted while in the Data Centers. No clients or visitors are granted unescorted access to the network operations center, UPS room, or generator area. Client access to Data Center facilities must be pre-authorized and visitors are met by TulsaConnect personnel outside of Data Center points of entry.

Facilities are accessed via a TulsaConnect escort, with the exception of authorized service personnel who are working on mechanical systems. Access codes are given to permanent electrical, HVAC, data cabling and other service vendors. This allows permanent vendors to address potential service impacting events while waiting for a TulsaConnect employee to arrive onsite. Access to the floor containing the Oklahoma City Data Center is restricted by elevator key code. The sites in Tulsa are similarly secured with escorted access.

When a facility entrance door is opened, a security device takes a series of pictures of the person(s) entering and exiting the Data Center and sends the time-stamped pictures to TulsaConnect staff via email. These logs are archived for 90 days. TulsaConnect Data Centers are monitored with video surveillance cameras that record on motion. This data is stored for at least 180 days.

LOGICAL SECURITY

Logical access to the LAN used to support the Data Center operations is restricted to authorized TulsaConnect personnel. A user ID and password combination is required to access network resources and file systems, and a VPN connection is required for remote access to the support network.

TulsaConnect personnel access is granted on a least privilege concept, and new user permissions are approved by an immediate supervisor. System Administrators are assigned unique user accounts, and default accounts are disabled or deleted. When an employee is terminated, their access revocation is confirmed by their immediate supervisor, and they are offboarded by the human resources department.

A password policy is in place to enforce the use of complex passwords. Passwords must be at least ten characters in length and include characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- base ten digits (zero through nine)
- nonalphanumeric characters

NETWORK SECURITY

The perimeter of the TulsaConnect support network is protected by a dedicated firewall. Data center traffic from the outside is routed to client specific subnets using external IP addresses. The client controls the rules below this initial routing. The firewall rule set has been configured in accordance with a default-deny concept. TulsaConnect's support network firewall utilizes antivirus, IPS, and geo-IP filtering technology as additional layers of protection.

Access to administrative functions on the TulsaConnect systems is restricted to authorized personnel. Remote access authorization is provided by the Director of Data Center Operations to TulsaConnect personnel with a supportable business need for remote access.

Access to TulsaConnect systems is segregated through the use of a network switching mechanism. Clients are connected to a routing switch. Each port is configured in a Layer 3 configuration, with the exception of clients with multiple ports in which case VLAN is created and the IP subnet is created on the VLAN interface.

Data center clients are assigned a unique IP subnet that does not overlap with other client subnets. Clients are provisioned on a separate switch port, which is configured in Layer 3 mode. An appropriately sized network block to meet client requirements is requested from the Director of Network Engineering, and clients are provided external IPs as required. The Director of Network Engineering determines which IP block to use and gives the information back to the System Administrator who requested it.

CHANGE MANAGEMENT

The primary contact mechanism for client support is via email. Issues submitted via email are documented, prioritized, and tracked through the ticketing system. Clients may also contact support via telephone. Client issues may require a follow-up email for documentation purposes. Additionally, planned

and emergency maintenance of facility-wide UPS systems are communicated to the client via email. Significant issues may be escalated using the established escalation policy within TulsaConnect's policies and procedures.

If an infrastructure change is required that would impact service availability to colocation clients, those changes are authorized by the Director of Data Center Operations or Director of Network Engineering. These changes are tested prior to implementation to minimize client impact.

SYSTEM MONITORING

An event that disrupts TulsaConnect's ability to serve its clients is classified as "disruptive." Any disruptive event is investigated and documented. The results of this investigation may result in an update to policy and procedure to minimize the chance of a similar event occurring.

Regular Data Center walkthroughs are performed to inspect for client server warning lights. Antivirus tools protect servers and network resources, administrative workstations, and Data Center networks. Incoming email messages are automatically scanned for virus and malware threats, and virus definitions are updated daily.

DATA BACKUP AND RECOVERY

Data backups are performed daily based on client specifications and detail reports are logged in a ticketing system. Backup job failures are logged by the backup software and are investigated in a timely manner. TulsaConnect personnel monitor the status of jobs on a routine basis. The backup software displays a report with the most recent backup success/failure status.

During the annual risk assessment, a tabletop exercise is conducted to test existing policies and procedures as they relate to business continuity and disaster recovery.

VENDOR MANAGEMENT

TulsaConnect monitors and evaluates third-party relationships to ensure vendor services and structural integrations align with and support Data Center service commitment requirements for security and availability. For select critical vendors who have access to the Data Center facility, a nondisclosure agreement is required.

COMPLEMENTARY USER ENTITY CONTROLS

TulsaConnect's system is designed with the assumption that certain controls will be implemented by the user entities of this report. Controls at TulsaConnect cover only a portion of a user entity's overall internal control environment, and it is not feasible for the objectives specified by TulsaConnect to be achieved solely by TulsaConnect. Therefore, a user entity's internal control environment must be evaluated in conjunction with TulsaConnect control activities and test results summarized in Section IV. The table below summarizes the types of controls which TulsaConnect expects user entities to implement and maintain in relation to the objectives within the scope of this report, but it should not be regarded as a comprehensive list of activities supporting the user entity's internal control environment.



Types of Control Activities TulsaConnect Expects to be Implemented by the User Entities	Applicable Objectives
User entities are responsible for notifying TulsaConnect in a timely manner of changes to personnel directly involved with services performed by TulsaConnect. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by TulsaConnect.	O5

USER ENTITY RESPONSIBILITIES

In addition to the complementary user entity control(s) above, there are certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

Types of Control Responsibilities TulsaConnect Expects to be Implemented by the User Entities	Applicable Objectives
User entities are responsible for implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for internal user entity components associated with TulsaConnect.	O5
User entities are responsible for implementing controls to ensure transactions made in connection to TulsaConnect services are appropriately authorized, secure, timely, and complete.	O5, O6
User entities are responsible for implementing controls to enforce approval procedures for critical transactions relating to TulsaConnect's services.	O5, O6
User entities are responsible for adhering to the terms and conditions stated in their contracts with TulsaConnect.	O6
User entities are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan that aids in the continuation of services provided by TulsaConnect.	O9
User entities are responsible for implementing controls to ensure IP assignments are working as expected, and that issues or concerns are communicated to TulsaConnect for resolution in a timely manner.	O5, O6

SIGNIFICANT CHANGES TO THE SYSTEM AND CONTROLS

TulsaConnect strives to continuously improve the processes, procedures, security posture, and internal control in support of the services provided to user entities as defined in this description. While some adjustments have been made, there were no significant changes that are likely to affect report users' understanding of how the Data Center hosting solutions system is used to provide the service during the period under examination for this report.

IDENTIFIED SYSTEM INCIDENTS

There were no identified system incidents that were the result of controls that were not suitably designed or operating effectively or otherwise resulted in a significant failure in the achievement of one or more of TulsaConnect's objectives during the period under examination.

IV. Control Objectives, Related Controls, and Control Test Procedures and Results

This section includes the objectives and related controls, both of which are the responsibility of TulsaConnect and are part of its system description. The control tests and results of tests are the responsibility of the service auditor. The tests performed include inquiry of appropriate personnel and corroboration with management; observation of the application, performance, or existence of the control; inspection of documents or reports indicating performance of the control; and/or reperformance of the control. In addition, HT evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Specified by TulsaConnect		Test Performed by HT	Test Results
1 - Controls provide reasonable assurance that management maintains segregation of duties and is responsible for oversight and consistent implementation of security practices.			
1.1	New employees acknowledge the confidentiality, privacy, and conduct responsibilities and requirements included in the Employee Handbook upon hire.	Selected a sample of new hires and inspected signature reports to verify the Employee Handbook was acknowledged upon hire.	No exceptions noted.
1.2	Management meets annually to update the risk assessment and review policies and procedures.	Inspected meeting minutes to verify management met to update the risk assessment and review policies and procedures.	No exceptions noted.
1.3	Organizational structure is grouped into functional areas to ensure adequate separation of duties around the management and processing of client information.	Inspected the organizational chart to verify separate functional areas supported sufficient segregation of duties within the organization.	No exceptions noted.
1.4	Employee responsibilities, business conduct, confidentiality requirements, privacy standards, and disciplinary action procedures are documented in the Employee Handbook.	Inspected the Employee Handbook to verify business conduct, confidentiality requirements, privacy standards, and disciplinary action procedures were formally documented.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
1.5	TulsaConnect policies and procedures are documented and maintained in a centralized employee-accessible knowledge base. Continued administration of the development, implementation, and maintenance of policies and procedures is the shared responsibility of the Director of Operations and other management personnel.	Inspected the Policies and Procedures Manual and the centralized knowledge base to verify policies and procedures were formally documented and maintained by the Director of Operations and/or other management personnel and were made available to employees.	No exceptions noted.
1.6	Management is responsible for business strategy, organizational objectives, delivery of services, and the design and implementation of information security controls, including an annual review of related policies and procedures.	Inspected the Policies and Procedures Manual to verify strategy, services, controls, and policies and procedures were reviewed and updated annually.	No exceptions noted.
1.7	Annual employee training includes HIPAA and security awareness.	Selected a sample of employees and inspected training reports to verify employees completed HIPAA and security awareness training.	No exceptions noted.
1.8	An annual risk assessment is performed by management to identify organizational objectives and risk rate threats to the objectives, including the consideration for potential fraud.	Inspected the annual risk assessment to verify risks to organizational objectives were identified, classified, and addressed, including the potential for fraud.	No exceptions noted.
1.9	Management meets annually to address organizational objectives and provide strategic direction.	Inspected meeting minutes to verify management met to address organizational objectives and provide strategic direction.	No exceptions noted.
1.10	Policies and procedures are documented and maintained to direct, guide, and authorize network security operations and monitoring.	Inspected the Policies and Procedures Manual to verify network security and monitoring policies and procedures were formally documented and maintained.	No exceptions noted.



Control Specified by TulsaConnect		Test Performed by HT	Test Results
2 - Controls provide reasonable assurance that employees understand their responsibilities and are suitable for the roles for which they are considered.			
2.1	New employees acknowledge the confidentiality, privacy, and conduct responsibilities and requirements included in the Employee Handbook upon hire.	Selected a sample of new hires and inspected signature reports to verify the Employee Handbook was acknowledged upon hire.	No exceptions noted.
2.2	Organizational structure is grouped into functional areas to ensure adequate separation of duties around the management and processing of client information.	Inspected the organizational chart to verify separate functional areas supported sufficient segregation of duties within the organization.	No exceptions noted.
2.3	Employee responsibilities, business conduct, confidentiality requirements, privacy standards, and disciplinary action procedures are documented in the Employee Handbook.	Inspected the Employee Handbook to verify business conduct, confidentiality requirements, privacy standards, and disciplinary action procedures were formally documented.	No exceptions noted.
2.4	Annual employee training includes HIPAA and security awareness.	Selected a sample of employees and inspected training reports to verify employees completed HIPAA and security awareness training.	No exceptions noted.
2.5	Systems administrators are evaluated on an annual basis to address individual performance and responsibilities.	Selected a sample of systems administrators and attempted to inspect annual evaluations to verify individual performance and responsibilities were reviewed.	Exceptions noted: For two of two system administrators selected, a performance evaluation was not completed during the period under examination.
2.6	Candidates are screened by TulsaConnect or a recruiter prior to hiring to confirm eligibility and qualifications.	Selected a sample of new hires and inspected background screening results to verify candidates were screened during the hiring process.	No exceptions noted.
2.7	Policies and procedures are documented and maintained to direct, guide, and authorize escalation procedures.	Inspected the Policies and Procedures Manual to verify procedures for addressing escalation procedures were formally documented and maintained.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
2.8	Job descriptions for employee positions are formally documented to define and communicate responsibilities, qualifications, and requirements.	Selected a sample of position titles and inspected job descriptions to verify responsibilities, qualifications, and requirements were formally documented.	No exceptions noted.
2.9	Policies and procedures are documented and maintained to direct, guide, and authorize change management operations.	Inspected the Policies and Procedures Manual to verify change management policies and procedures were formally documented and maintained.	No exceptions noted.
2.10	Policies and procedures are documented and maintained to direct, guide, and authorize data backup, replication, and recovery.	Inspected the Policies and Procedures Manual to verify data backup, replication, and recovery policies and procedures were formally documented and maintained.	No exceptions noted.
2.11	TulsaConnect has incident response policies for potentially disruptive events.	Inspected incident response policies to verify procedures for addressing potentially disruptive events were formally documented and maintained.	No exceptions noted.
3 - Controls provide reasonable assurance that physical assets are adequately protected against environmental hazards and related damage, and that physical access to the computer equipment, system infrastructure, and storage media is limited to authorized personnel.			
3.1	Data centers are designed for and feature redundant HVAC units, which are properly maintained.	Observed Data Center facilities and inspected service work orders to verify redundant HVAC units were operating and properly maintained.	No exceptions noted.
3.2	Client equipment in Data Center areas is secured in locked cabinets.	Inspected locked rack cabinets at each Data Center location to verify access to client equipment was secure and restricted by key lock.	No exceptions noted.
3.3	Data centers and critical systems in administrative offices are equipped with UPS units, which are properly maintained.	Observed Data Center facilities and inspected annual UPS preventative maintenance reports to verify UPS units were in place and were maintained in accordance with equipment service plans.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
3.4	TulsaConnect Data Centers are monitored with video surveillance cameras that record on motion and store images for at least 180 days.	Observed cameras and inspected Data Center surveillance files for each location to verify video surveillance was in place and recordings were stored for at least 180 days.	No exceptions noted.
3.5	Policies and procedures are documented and maintained to direct, guide, and authorize physical security.	Inspected the Policies and Procedures Manual to verify physical security policies and procedures were formally documented and maintained.	No exceptions noted.
3.6	Data centers are equipped with fire detection and suppression devices, including annually serviced fire extinguishers.	Observed Data Center facilities and inspected fire extinguisher maintenance tags at each Data Center to verify fire sensors and inert gas fire suppression systems were in place and equipment was inspected and properly maintained.	No exceptions noted.
3.7	External generator connection points for a trailer-mounted diesel generator are installed on the outside of each Data Center building in the event of a primary generator failure.	Observed external generator connections to verify secondary emergency power points were in place at each Data Center.	No exceptions noted.
3.8	Environmental sensors are installed in the Data Centers and send alerts based on parameters for motion, temperature, humidity, air flow, and door position.	Observed Data Center facilities and inspected NetBotz unit monitoring and alert configurations to verify environmental sensors were installed in each Data Center.	No exceptions noted.
3.9	Onsite emergency generators are in place and properly maintained to supply full load electrical power in the event of a public utility power grid failure.	Observed onsite emergency generators and inspected generator maintenance checklists for each location to verify equipment was in place, and maintenance and repairs were performed.	No exceptions noted.
3.10	Onsite emergency generators are automatically tested on a weekly basis.	Selected a sample of weeks and inspected email alerts for each Data Center to verify generators were tested weekly.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
3.11	When a facility entrance door is opened, a security device takes a series of pictures of the area and sends the time-stamped images to TulsaConnect NOC staff via email. These logs are archived for 90 days.	Selected a sample of dates from the last 90 days of the period and inspected email notifications to verify door alerts for each Data Center were logged and stored.	No exceptions noted.
3.12	Data center entrances require biometric identification of TulsaConnect personnel.	Observed the use of biometric door locks at each Data Center location to verify access was restricted to personnel with authorized biometrics.	No exceptions noted.
3.13	Client and vendor access to Data Center facilities is pre-authorized and visitors are met by TulsaConnect personnel outside of Data Center points of entry to be escorted into the Data Center.	Observed facility entrances and discussed with management to verify that visitor access was escorted by TulsaConnect personnel.	No exceptions noted.
3.14	Generator service vendor is required to test the generator after maintenance is performed.	Inspected generator maintenance checklists for each Data Center to verify testing occurred on generators after maintenance was performed.	No exceptions noted.
3.15	User physical and logical access is revoked upon termination and tracked in a checklist.	Selected a sample of terminated employees and inspected offboarding documentation and user access listings to verify access was tracked and removed.	No exceptions noted.
4 - Controls provide reasonable assurance that system availability is maintained and that systems operate in a consistent and predictable manner.			
4.1	Walkthroughs of the Data Centers to look for server warning lights are performed on a daily basis.	Selected a sample of days and inspected task lists for each Data Center to verify onsite monitoring inspections were performed and documented.	No exceptions noted.
4.2	Policies and procedures are documented and maintained to direct, guide, and authorize system availability and Data Center facility operations in a consistent, predictable manner.	Inspected the Policies and Procedures Manual to verify system availability and Data Center operations policies and procedures were formally documented and maintained.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
4.3	Data centers and critical systems in administrative offices are equipped with UPS units, which are properly maintained.	Observed Data Center facilities and inspected annual UPS preventative maintenance reports to verify UPS units were in place and were maintained in accordance with equipment service plans.	No exceptions noted.
4.4	Environmental sensors are installed in the Data Centers and send alerts based on parameters for motion, temperature, humidity, air flow, and door position.	Observed Data Center facilities and inspected NetBotz unit monitoring and alert configurations to verify environmental sensors were installed in each Data Center.	No exceptions noted.
4.5	Onsite emergency generators are in place and properly maintained to supply full load electrical power in the event of a public utility power grid failure.	Observed onsite emergency generators and inspected generator maintenance checklists for each location to verify equipment was in place, and maintenance and repairs were performed.	No exceptions noted.
4.6	Generator service vendor is required to test the generator after maintenance is performed.	Inspected generator maintenance checklists for each Data Center to verify testing occurred on generators after maintenance was performed.	No exceptions noted.
4.7	A tool is used to monitor activity and alert for issues.	Inspected monitoring configurations and ticket documentation to verify a tool was used to monitor activity and alert for vulnerabilities or issues.	No exceptions noted.
4.8	Data centers are designed for and feature redundant HVAC units, which are properly maintained.	Observed Data Center facilities and inspected service work orders to verify redundant HVAC units were operating and properly maintained.	No exceptions noted.
4.9	Onsite emergency generators are automatically tested on a weekly basis.	Selected a sample of weeks and inspected email alerts for each Data Center to verify generators were tested weekly.	No exceptions noted.

Control Specified by TulsaConnect		Test Performed by HT	Test Results
4.10	External generator connection points for a trailer-mounted diesel generator are installed on the outside of each Data Center building in the event of a primary generator failure.	Observed external generator connections to verify secondary emergency power points were in place at each Data Center.	No exceptions noted.
5 - Controls provide reasonable assurance that logical access to programs, data, and operating systems is restricted to authorized personnel.			
5.1	Logical access to Data Center operations systems is restricted to authorized TulsaConnect personnel based on individual roles and responsibilities.	Inspected user access listings and account permissions to verify logical access was restricted to authorized personnel.	No exceptions noted.
5.2	New users are granted physical and logical access based on approval by authorized personnel.	Selected a sample of new users and inspected an onboarding checklist to verify access provisioned was approved by authorized personnel.	No exceptions noted.
5.3	Policies and procedures are documented and maintained to direct, guide, and authorize logical security and user access provisioning.	Inspected the Policies and Procedures Manual to verify logical security policies and procedures were formally documented and maintained.	No exceptions noted.
5.4	System Administrators are assigned unique user accounts on the TulsaConnect support network and administrative functions are restricted to authorized personnel.	Inspected user listings to verify system administrators were assigned unique user accounts and administrative functions were restricted to authorized personnel.	No exceptions noted.
5.5	The TulsaConnect Active Directory security policy is configured to enforce password length, complexity, expiration, and history requirements.	Inspected the default domain policy to verify password length, complexity, expiration, and history requirements were configured.	No exceptions noted.
6 - Controls provide reasonable assurance that network security and monitoring procedures are in place to identify and report unauthorized access attempts, and that clients understand the limits of the TulsaConnect service and their responsibility to implement network security controls.			
6.1	Firewall rulesets are configured in accordance with a default-deny concept.	Inspected firewall rulesets for each Data Center location to verify dedicated firewalls were configured in accordance with a default-deny concept.	No exceptions noted.

Control Specified by TulsaConnect		Test Performed by HT	Test Results
6.2	The perimeter of the TulsaConnect support network is protected by a dedicated firewall.	Inspected firewall rulesets for each Data Center location to verify dedicated firewalls were in place to protect the TulsaConnect support network.	No exceptions noted.
6.3	Policies and procedures are documented and maintained to direct, guide, and authorize network-level security for client services.	Inspected the Policies and Procedures Manual to verify network-level security authorization policies and procedures for client services were formally documented and maintained.	No exceptions noted.
6.4	Prior to the deployment of new client services, the rights, requirements, and responsibilities of the client and TulsaConnect are clearly communicated through the signing of a Master Service Agreement.	Selected a sample of new clients and inspected signed Master Service Agreements to verify rights, requirements, and responsibilities were documented and communicated.	No exceptions noted.
6.5	TulsaConnect systems access is designed to be segregated through the use of a network switch.	Inspected the network diagram to verify system access was segregated through the use of a network switch.	No exceptions noted.
6.6	Client data environments are logically segregated and Data Center clients are assigned unique IP subnets.	Inspected the network diagram to verify client data environments were logically segregated. Selected a sample of new Data Center clients and inspected maintenance dashboards to verify unique IP addresses were provisioned for each client.	No exceptions noted. No exceptions noted.
6.7	Policies and procedures are documented and maintained to direct, guide, and authorize escalation procedures.	Inspected the Policies and Procedures Manual to verify procedures for addressing escalation procedures were formally documented and maintained.	No exceptions noted.
6.8	Policies and procedures are documented and maintained to direct, guide, and authorize network security operations and monitoring.	Inspected the Policies and Procedures Manual to verify network security and monitoring policies and procedures were formally documented and maintained.	No exceptions noted.



<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
6.9	A tool is used to monitor activity and alert for issues.	Inspected monitoring configurations and ticket documentation to verify a tool was used to monitor activity and alert for vulnerabilities or issues.	No exceptions noted.
6.10	Antivirus tools protect servers and network resources, administrative offices, and Data Center networks.	Inspected network security application system configurations for all locations to verify antivirus tools were in place.	No exceptions noted.
6.11	Incoming email messages are automatically scanned for virus and malware threats.	Inspected antivirus tool configurations to verify incoming email messages were automatically scanned for virus and malware threats.	No exceptions noted.
7 - Controls provide reasonable assurance that systems, processes, and software are tested periodically to ensure that security is maintained over time and after changes.			
7.1	Colocation customer impacting changes to power, infrastructure, and distribution networks are authorized and tested.	Attempted to select a sample of colocation customer impacting changes to verify changes to power, infrastructure, and distribution networks were authorized and tested.	Not tested: Per discussion with management, no colocation customer impacting changes occurred during the period under examination.
7.2	Walkthroughs of the Data Centers to look for server warning lights are performed on a daily basis.	Selected a sample of days and inspected task lists for each Data Center to verify onsite monitoring inspections were performed and documented.	No exceptions noted.
7.3	Management meets annually to update the risk assessment and review policies and procedures.	Inspected meeting minutes to verify management met to update the risk assessment and review policies and procedures.	No exceptions noted.
7.4	Onsite emergency generators are automatically tested on a weekly basis.	Selected a sample of weeks and inspected email alerts for each Data Center to verify generators were tested weekly.	No exceptions noted.
7.5	Management meets annually to address organizational objectives and provide strategic direction.	Inspected meeting minutes to verify management met to address organizational objectives and provide strategic direction.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
7.6	An annual tabletop exercise is performed to evaluate business continuity and disaster recovery procedures.	Inspected tabletop exercise results and meeting minutes to verify business continuity and disaster recovery procedures were tested and evaluated.	No exceptions noted.
7.7	Policies and procedures are documented and maintained to direct, guide, and authorize system monitoring operations.	Inspected the Policies and Procedures Manual to verify system monitoring policies and procedures were formally documented and maintained.	No exceptions noted.
7.8	Generator service vendor is required to test the generator after maintenance is performed.	Inspected generator maintenance checklists for each Data Center to verify testing occurred on generators after maintenance was performed.	No exceptions noted.
8 - Controls provide reasonable assurance that routine, client-requested, and emergency change management issues are communicated to the client.			
8.1	TulsaConnect has incident response policies for potentially disruptive events.	Inspected incident response policies to verify procedures for addressing potentially disruptive events were formally documented and maintained.	No exceptions noted.
8.2	Technical staff are notified in the event of a power blip, if a generator starts, or if other significant events occur.	Inspected email alerts to verify technical staff were notified of significant events to the generator.	No exceptions noted.
8.3	Policies and procedures are documented and maintained to direct, guide, and authorize escalation procedures.	Inspected the Policies and Procedures Manual to verify procedures for addressing escalation procedures were formally documented and maintained.	No exceptions noted.
8.4	Client issues submitted via email and phone are tracked through a customer support application.	Selected a sample of client support tickets and inspected ticket documentation to verify issues were tracked in a customer support application.	No exceptions noted.
8.5	Planned and emergency maintenance of the facility-wide UPS system is communicated to clients via email.	Inspected email notifications to verify planned and emergency maintenance of the facility-wide UPS system was communicated with clients.	No exceptions noted.

<i>Control Specified by TulsaConnect</i>		<i>Test Performed by HT</i>	<i>Test Results</i>
8.6	Policies and procedures are documented and maintained to direct, guide, and authorize change management operations.	Inspected the Policies and Procedures Manual to verify change management policies and procedures were formally documented and maintained.	No exceptions noted.
9 - Controls provide reasonable assurance that data is backed up in a secure manner for offsite retrieval and backup details are logged.			
9.1	Data backups are performed daily and detail reports are logged in a ticketing system.	Selected a sample of days and servers and inspected backup summary reports to verify data backups were performed and details were logged.	No exceptions noted.
9.2	Policies and procedures are documented and maintained to direct, guide, and authorize data backup, replication, and recovery.	Inspected the Policies and Procedures Manual to verify data backup, replication, and recovery policies and procedures were formally documented and maintained.	No exceptions noted.
9.3	An annual tabletop exercise is performed to evaluate business continuity and disaster recovery procedures.	Inspected tabletop exercise results and meeting minutes to verify business continuity and disaster recovery procedures were tested and evaluated.	No exceptions noted.

V. Other Information Provided by MBO Data, LLC dba TulsaConnect

MANAGEMENT'S RESPONSES TO EXCEPTIONS IDENTIFIED DURING TESTING

<i>Objective</i>	<i>Control Specified by TulsaConnect</i>	<i>Test Results</i>	<i>Management's Response</i>
CO2	Systems administrators are evaluated on an annual basis to address individual performance and responsibilities.	Exceptions noted: For two of two system administrators selected, a performance evaluation was not completed during the period under examination.	Evaluations were not performed on these particular individuals as MBO Companies was in the process of implementing a new Performance Review system. Their supervisor at the time was told to wait to perform the evaluations until the new system was in place. This system was not implemented completely until after the period under examination.

Glossary of Abbreviations and Terminologies

CPU	Central Processing Unit
DC	Data Center
HIPAA	Health Insurance Portability and Accountability Act
HT	HoganTaylor LLP
HVAC	Heating, ventilation, and air conditioning
ID	Identification
IP	Internet protocol
IPS	Intrusion prevention system
IT	Information technology
LAN	Local area network
NOC	Network operations center
OS	Operating system
SOC	System and Organization Controls
UPS	Uninterruptible power supply
VLAN	Virtual local area network
VM	Virtual machines
VPN	Virtual private network