EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and __A+ Technology & Security Solutions, Inc______________________ (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Ulster County BOCES ("BOCES") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that Ulster County BOCES' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by Ulster County BOCES. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of Ulster County BOCES as that term is defined in § 99.3 of FERPA,

-AND-

> Personally identifiable information from the records of Ulster County BOCES 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with Ulster County BOCES policy(ies) on data security and privacy. Contractor shall promptly reimburse Ulster County BOCES for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of Ulster County BOCES' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of Ulster County BOCES' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to Ulster County BOCES, transitioned to a successor contractor, at Ulster County BOCES' option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of Ulster County BOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

   a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
   b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, BOCES board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of Ulster County BOCES' Parent Bill of Rights.

NAME OF PROVIDER:___A+ Technology & Security Solutions, Inc,______________________________

BY: ______________________________ DATED: ___3/12/23___________________

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Shared Vision
Shared Commitment
Shared Success
ULSTER
BOCES
Board of Cooperative Educational Services

PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Ulster BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law §2-d, Ulster BOCES wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to:

   Ulster BOCES
   175 Route 32 North
   New Paltz, New York 12561

   or

   Chief Privacy Officer
   New York State Education Department
   89 Washington Avenue
   Albany, New York 12234

   Complaints may also be directed to the
   Chief Privacy Officer (CPO) via e-mail at
   CPO@mail. nysed.gov

6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data as well as teacher or principal data.

Supplemental Information Regarding Third Party Contractors

In the course of complying with its obligations under the law and providing educational services, Ulster BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract Ulster BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1. The exclusive purposes for which the student data or teacher or principal data will be used by third party contractor;

2. How the third party contractor will ensure that the subcontractors, persons or entities with whom the third party contractor will disclose the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

3. The duration of the contract, including when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.

6. Address how the data will be protected using encryption while in motion and at rest.

Signature: ______________________

Print Name: David Antar

Title: President

Company Name: A+ Technology & Security Solutions Inc

Date: 3/12/23

DATA PRIVACY AND SECURITY AGREEMENT

WHEREAS, *A+ Technology & Security Solutions Inc*, having its principle address at *1490 N Clinton Rd Bayshore NY 11706* (hereinafter "Contractor") and the Board of Cooperative Educational Services, local education agency (LEA) (hereinafter "LEA"), collectively "the Parties," are parties to an agreement through which Contractor will provide LEA with *Technology Services and Software*; and

WHEREAS, pursuant to that agreement, Contractor will receive student data and/or teacher or principal data in possession of LEA and/or its officers, employees, agents, and students, and may also receive student data and/or teacher or principal data of educational agencies within New York State that contract with LEA for the use of Contractor's products and/or services; and

WHEREAS, in conformance with N.Y. Education Law § 2-d and 8 N.Y.C.R.R. § 121.1, *et seq*., the Parties enter into this Data Privacy and Security Agreement (hereinafter the "Agreement") to address the confidentiality and security of student data and/or teacher or principal data received by Contractor.

NOW, THEREFORE, the Parties agree as follows:

1. For purposes of this Agreement, terms shall be defined as follows:

   a. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

   b. "Commercial Purpose" or "Marketing Purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.

   c. "Disclose" or "Disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

   d. "Education Records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

   e. "Eligible Student" means a student who is eighteen years or older.

   f. "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

g. “Parent” means a parent, legal guardian, or person in parental relation to a student.

h. “Personally Identifiable Information,” as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).

i. “Release” shall have the same meaning as Disclosure or Disclose.

j. “Student” means any person attending or seeking to enroll in an educational agency.

k. “Student data” means personally identifiable information from the student records of an educational agency. For purposes of this agreement, “student data” includes information made accessible to Contractor by LEA, LEA officers, LEA employees, LEA agents, LEA students, and/or the officers, employees, agents, and/or students of educational agencies with whom LEA contracts.

l. “Teacher or principal data” means 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 N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this agreement, “teacher or principal data” includes information made accessible to Contractor by LEA, LEA officers, LEA employees, LEA agents, LEA students, and/or the officers, employees, agents, and/or students of educational agencies with whom LEA contracts.

m. “Unauthorized Disclosure” or “Unauthorized Release” means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

2. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with:

a. Applicable state and federal laws that protect the confidentiality of personally identifiable information;

b. The terms and conditions of this Agreement, including but not limited to the LEA Parents Bill of Rights for Data Security and Privacy and the Supplemental Information to Parents Bill or Rights for Data Privacy and Security, attached hereto as Exhibit A; and

c. Applicable LEA policies, which can be accessed on the LEA website at: https://go.boarddocs.com/ny/LEA/Board.nsf/Public.

3. Contractor will not use subcontractors in fulfilling its responsibilities to LEA, its employees or agents, and/or educational agencies which contract with LEA for the provision of Contractor's products and/or services. Contractor will not use sub-contractors to deliver services. Contractor will use A+ Virtual instructors and will manage relationships through direct contractual agreements between A+ Technology & Security Solutions Inc and its instructors . All instructors are obligated contractual to privacy agreements and the delivery of services will be limited to and only via A+ Virtual classrooms.

4. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers, employees, agents, subcontractors, and/or assignees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to that data. Training is provided to A+ Virtual Instructors upon hire and at regular intervals to maintain their understanding of data security and protections requirements.

5. The exclusive purpose for which Contractor is being provided student data and/or teacher or principal data, and for which such information will be used, is to provide the products and services LEA has contracted for.

6. Student data and/or teacher or principal data received by Contractor, or by any subcontractor or assignee of Contractor, shall not be sold or used for marketing purposes.

7. The agreement between Contractor and LEA for products and/or services expires on *6/27/23*. Upon expiration of that agreement without a successor agreement in place, Contractor shall assist LEA and any educational agencies that contracts with LEA for the provision of Contractor's products or services in exporting any and all student data and/or teacher or principal data previously received by Contractor back to LEA or the educational agency that generated the student data and/or principal data. Contractor shall thereafter securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within 30 days of the expiration of the agreement between LEA and Contractor, and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue

to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to LEA from an appropriate officer that the requirements of this paragraph have been satisfied in full.

8. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by LEA or the educational agency that generated the student data for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the applicable educational agency's Annual Professional Performance Review Plan.

9. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States, or a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily be limited to disk encryption, file encryption, firewalls, and password protection. A+ Virtual and related companies are supported by a team of IT professionals utilizing the full suite of Kaseya cyber security products and undergoes regular testing of network, virus protection updates.

10. Contractor acknowledges that it has the following obligations with respect to any student data and/or teacher or principal data provided pursuant to its agreement with LEA, and any failure to fulfill one of these obligations set forth in New York State Education Law § 2-d and/or 8 N.Y.C.R.R. Part 121 shall also constitute a breach of its agreement with LEA:

a. Limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of § 2-d and the Family Educational Rights and Privacy Act;

b. Not use education records/and or student data for any purpose other than those explicitly authorized in this Agreement;

c. Not disclose any personally identifiable information to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under this Agreement, unless (i) that other party has the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

d. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;

e. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

f. Notify LEA of any breach of security resulting in an unauthorized release of student data by Contractor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but not more than seven (7) calendar days after discovery of the breach;

g. Where a breach or unauthorized release of personally identifiable information is attributable to Contractor, Contractor will pay or reimburse LEA and/or any educational agencies which contract with LEA for the provision of Contractor's products or services for the cost of any notifications LEA and/or such other educational agencies is/are required to make by applicable law, rule, or regulation; and

h. Contractor will cooperate with LEA and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.

i. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on Contractor by state and federal law, and by this Agreement, shall apply to the subcontractor.

11. In the event of a data security and privacy incident (including but not limited to a breach, unauthorized release, and/or unauthorized disclosure) implicating the personally identifiable information of students, teachers, and/or principals of LEA or educational agencies which contract with LEA for the provision of Contractor's products or services, Contractor will:

a. A+ Technology & Security Solutions Inc incorporates the full suite of Kaseya cyber security products to deter, prevent and remediate potential network breaches;

b. Notify LEA in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and paragraph 10(f), above.

12. Contractor, its employees and representatives shall at all times comply with all applicable federal, state, and local laws, rules, and regulations.

13. This Agreement, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, constitutes the entire understanding of the Parties with respect to the subject matter thereof. The terms of this Agreement, together with the signed Parents Bill of Rights for Data Privacy and the

Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, shall supersede any conflicting provisions of Contractor’s terms of service or privacy policy.

14. If any provision of this Agreement shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision to this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

15. This Agreement shall be binding on any successors of the parties. Neither party shall have the right to assign its interests in the Agreement to any other party, unless the prior written consent of the other party is obtained.

16. This Agreement shall be governed by the laws of the State of New York. Any action or proceeding arising out of this contract shall brought in the appropriate courts of New York State.

In witness of the foregoing, the duly authorized representatives of the Parties have signed this Memorandum on the date indicated.

FOR THE CONTRACTOR:
A+ Technology & Security Solutions Inc,

____
David Antar
President

3/13/23
____
Date

EXHIBIT A: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

LEA is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, LEA wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be submitted to NYSED at www.nysed.gov/data-privacy-security; by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

Supplemental Information to Parents Bill or Rights for Data Privacy and Security:

1. The exclusive purpose for which Contractor is being provided access to student data and/or teacher or principal data is Virtual Classroom instruction. Student data and/or teacher or principal data received by Contractor, or by any assignee of Contractor, from LEA or its employees, officers, agents, and/or students will not be sold or used for marketing purposes.

2. Contractor agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. More specifically, All administrative and instruction personal receive initial and ongoing training to ensure they abide by data protection and security requirements best practices.

2. The agreement between Contractor and LEA for Virtual Classroom Instruction expires on 6/27/23. Upon expiration of that agreement without a successor agreement in place, Contractor will assist LEA in exporting any and all student data and/or teacher or principal data previously received by Contractor back to LEA. Contractor will thereafter securely delete any and all student data and/or teacher or principal data remaining in its possession or the possession of its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data), as well as any and all student data and/or teacher or principal data maintained on its behalf of in secure data center facilities. Contractor will ensure that no copy, summary, or extract of the student data and/or teacher or principal data, or any related work papers, are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within thirty (30) days of the expiration of the agreement between BOCES and Contractor. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they/it will not attempt to re-identify de-identified data and will not transfer de-identified data to any party.

3. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the LEA for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that a teacher or principal wishes to challenge the accuracy of the teacher or principal data that is collected, he or she may do so consistent with applicable provisions of 8 N.Y.C.R.R. Part 30 and the BOCES Annual Professional Performance Review Plan.

4. Student data and/or teacher or principal data transferred to Contractor by LEA or LEA officers, employees, agents, or students will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection. A+ Technology & Security Solutions Inc utilizes a full suite of cyber security products from Kaseya.

4. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption while in motion and at rest

Acknowledged and agreed to by:

Signature: ______________________________

Name: David Antar ______________________________

Title: President______________________________

Date: 3/13/23______________________________