

CONTRACT AMENDMENT NO. 1

1. PARTIES

This Amendment to the above-referenced Original Contract (hereinafter called the "Contract") is entered into by and between Augenblick, Palaich and Associates, Inc., 1120 Lincoln St., Suite 1101, Denver, CO 80203, (hereinafter called "Contractor"), and the STATE OF COLORADO, acting by and through the Colorado Department of Education, 201 East Colfax, Denver, Colorado 80203 (hereinafter called "Department" or "State.")

2. EFFECTIVE DATE AND ENFORCEABILITY

This Amendment shall not be effective or enforceable until it is approved and signed by the Colorado State Controller or designee (hereinafter called the "Effective Date.") The Department shall not be liable to pay or reimburse Contractor for any performance hereunder, including, but not limited to, costs or expenses incurred, or be bound by any provision hereof prior to the Effective Date.

3. FACTUAL RECITALS

The Parties entered into the Contract for Contractor to provide the research design for the evaluation component of the "Right 4 Rural" grant, an essential component of the grant's proposal. Also, CDE is seeking guidance in data collection, data analysis of surveys, and annual reporting of grant progress and final results related to identification of underrepresented students in gifted education in rural settings. The purpose of this Amendment is to extend the Contract to August 31, 2017 and to update the privacy and security language to comply with 22-16-101 et. al., C.R.S.

4. CONSIDERATION

The Parties acknowledge that the mutual promises and covenants contained herein and other good and valuable consideration are sufficient and adequate to support this Amendment.

5. LIMITS OF EFFECT

This Amendment is incorporated by reference into the Contract, and the Contract and all prior amendments thereto, if any, remain in full force and effect except as specifically modified herein.

6. MODIFICATIONS

The Contract and all prior amendments thereto, if any, are modified as follows:

- A. Section IV. Definitions, the following definitions are deleted as they are now redefined in Section X or not used in the Contract: "Covered Information," "Incident," "Personally Identifiable Information (PII) Data," "State Confidential Information," "Student Data," "State Information," "State Records," and "Summary or De-identified Data."
- B. Section V. Term, Subsection A. Initial Term-Work Commencement is hereby amended to extend the termination date of the Contract to August 31, 2017. The Section is amended to state:

A. Initial Term-Work Commencement

The Parties' respective performances under this Contract shall commence on the later of either the Effective Date or May 09, 2016. This Contract shall terminate on August 30, 2017 unless sooner terminated or further extended as specified elsewhere herein.

- C.** The table in Section VII. Payments to Contractor, Subsection A. Maximum Amount remains the same. The table is as follows:

Grant Year 1 (Effective Date thru August 31, 2016)	\$39,650.00
Additional Deliverables To Be Performed Throughout All Grant Years (All Funds To Be Encumbered in Initial Grant Year)	\$8,500.00
Grant Year 2 (September 01, 2016 thru August 31, 2017)	\$33,608.00
Grant Year 3 (September 01, 2017 thru August 31, 2018)	\$37,670.00
Total for all Three Years	\$119,428.00

- D.** Section X, Confidential Information-State Records is hereby deleted in its entirety and replaced with the following:

X. CONFIDENTIAL INFORMATION

A. Definitions

1. "Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.
2. "Destroy" means to remove Student Personally Identifiable Information from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in NIST Special Publication 800-88 Guidelines for Media Sanitization so that the Student Personally Identifiable Information is permanently irretrievable in the Contractor's and Subcontractor's normal course of business.
3. "Incident" means an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State pursuant to C.R.S. Section 24-37.5-401 et seq. Incidents include, but are not limited to (i) successful attempts to gain unauthorized access to a State system or Student Personally Identifiable Information or State Confidential Information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; or (iv) changes to State system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent.

4. "State Confidential Information" means all information, data, records, and documentary materials, regardless of physical form or characteristics, which are of a sensitive nature and belong to the State, including but not limited to any non-public State records, sensitive State data, protected State data, State personnel records and other information or data concerning individuals, which has been communicated, furnished, or disclosed by the State to Contractor. Notwithstanding the foregoing, State Confidential Information shall not include Student Personally Identifiable Information and shall not include information required to be disclosed pursuant to the Colorado Open Records Act, CRS §24-72-101, et seq.
5. "Student Personally Identifiable Information (PII)" means information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent or family. Student Personally Identifiable Information includes, but is not limited to a student's name; the name of a student's parent or other family member; the address of a student or student's family; a personal identifier such as a student's social security number, student number, or biometric record; other indirect identifiers such as a student's date of birth, place of birth, and mother's maiden name; a student's email address, cell phone number or any other information that allows physical or online contact with a student; a student's discipline or criminal records; a student's juvenile dependency records; a student's medical or health records including, without limitation, records regarding a student's disabilities; a student's socioeconomic information, political affiliations, or religion; a student's text messages, IP address, or online search activity; a student's photos and voice recordings; a student's food purchases; or geolocation information.
6. "Subcontractor" means any third party engaged by Contractor to aid in performance of Contractor's obligations.
7. "Targeted Advertising" means selecting and sending advertisements to a student based on information obtained or inferred over time from the student's online behavior, use of applications, or PII. Targeted Advertising does not include advertising to a student at an online location based on the student's current visit to that location or in response to the student's request for information or feedback and is without the collection and retention of a student's online activities over time. Targeted Advertising also does not include adaptive learning, personalized learning, or customized education.

B. General Provisions

1. The State reserves all right, title, and interest, including all intellectual property and proprietary rights, in and to system data, State Confidential Information, PII, and all related data and content.
2. Contractor shall comply with all laws and regulations concerning confidentiality of State Confidential Information and PII. Contractor shall immediately forward to the State's principal representative any request or demand from a third party for State Confidential Information or PII in the possession of Contractor.
3. Upon request of the State or of the Colorado State Board of Education, Contractor shall submit its data processing facilities for an audit of the measures referred to in this Section

X by the State or by a State approved delegate.

4. Contractor shall send the State a written notice which includes a clear explanation of the proposed changes prior to making a material change to Contractor's privacy policies.

C. Confidentiality of State Confidential Information

1. Contractor shall notify its agents, employees, Subcontractors, and assigns who may come into contact with State Confidential Information that each is subject to the confidentiality requirements set forth in this Contract, and shall provide each with a written explanation of such requirements before permitting them to access State Confidential Information.
2. State Confidential Information shall not be distributed or sold to any third party or used by Contractor or its agents except as authorized by this Contract or as approved in writing by the State. Contractor shall provide and maintain a secure environment that ensures confidentiality of all State Confidential Information wherever located. State Confidential Information shall not be retained by Contractor or its agents except as permitted in this Contract or approved in writing by the State.
3. Disclosure of State Confidential Information by Contractor for any reason may be cause for legal action by third parties against Contractor, the State or their respective agents. Contractor shall indemnify, save, and hold harmless the State, its employees and agents, against any and all costs, expenses, claims, damages, liabilities, and court awards (including attorney fees and costs), incurred by the State in relation to any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees in connection with State Confidential Information.

D. Subcontractors

1. Contractor shall not use a Subcontractor or disclose PII to a Subcontractor unless and until the Contractor contractually requires the Subcontractor to comply with C.R.S. §§22-16-108 through 22-16-111 and the requirements of this Section X.
2. If Contractor discovers that Subcontractor or any subsequent subcontractor has committed a material breach of the contract between Contractor and Subcontractor that involves the misuse or unauthorized release of PII, Contractor acknowledges that the State may terminate the Contract with Contractor unless Contractor terminates the contract with Subcontractor as soon as possible after Contractor knows or has reason to know of Subcontractors' or any subsequent subcontractors' material breach.
3. Upon discovering the misuse or unauthorized release of PII held by a Subcontractor or any subsequent Subcontractor, Contractor shall notify CDE and the Office of Information Security ("OIS") within one calendar day, regardless of whether the misuse or unauthorized release by the Subcontractor is a result of a material breach of the terms of the Contract or results in an Incident.
4. No later than thirty (30) days after the signing of this Contract, Contractor shall provide the State with information detailing the purpose and the scope of the contract between the

Contractor and all Subcontractor(s) and the types and uses of PII that Subcontractor(s) holds under the Contract between the Contractor and Subcontractor(s).

5. Contractor shall not maintain or forward PII to or from any other facility or location except for backup and disaster recovery purposes. Any backup or disaster recovery contractor shall be considered a Subcontractor that must comply with the Subcontractor requirements in this Section X.

E. End of Agreement

1. Should Contractor not comply with the requirements of this Section and that non-compliance results in the misuse or unauthorized release of PII by the Contractor, the State may terminate the Contract immediately as provided under this Contract and in accordance with C.R.S. Section 22-16-105(5).
2. Upon request by the State made before or within thirty (30) calendar days after termination of the Contract, Contractor shall make available to the State a complete and secure (i.e. encrypted and appropriately authenticated) download file of all data, including, but not limited to, all PII, State Confidential Information, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format.
3. Following the termination of this Contract, Contractor shall, within thirty (30) calendar days, Destroy all PII and State Confidential Information collected, generated, or inferred as a result of this Contract. The Contractor shall notify the State of the date upon which all of the PII and State Confidential Information is Destroyed.
4. The State retains the right to use the established operational services to access and retrieve PII and State Confidential Information stored on Contractor's infrastructure at its sole discretion.

F. Use

1. The Contractor shall not use or share PII beyond the purposes set forth as follows:
 - (a) To carry out the Contractor's responsibilities listed in Exhibit A, Statement of Work.
2. In the event the Contract requires Contractor to store, process or transfer PII, Contractor shall store, process, and transfer PII only in or to facilities located within the United States.
3. During the term of this Contract, if the State requests the destruction of a student's PII collected, generated or inferred as a result of this Contract, the Contractor shall Destroy the information within five (5) calendar days after the date of the request unless:
 - (a) The Contractor obtains the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian to retain the student's PII; or
 - (b) The student has transferred to another state and the receiving state has requested that the Contractor retain the student's PII.

4. If Contractor seeks to share or publically release PII without complying with the requirements of this Section X for Subcontractors, Contractor must de-identify or aggregate the PII prior to providing that information to a third party or releasing the data publically. For data that is de-identified or aggregate, the following requirements apply:
 - (a) PII that must be aggregated or de-identified shall include not only direct identifiers, such as names, student IDs or social security numbers, but also any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification.
 - (b) Simple removal of direct identifiers from the data to be released shall not constitute adequate de-identification.
 - (c) Contractor shall de-identify data to remove cumulative re-identification risks.
 - (d) Contractor shall remove all PII that in conjunction with previous data releases and other reasonably available information, including publicly-available directory information and de-identified data releases from education records and other sources, would allow for identification of a particular student.
 - (e) Contractor shall have specific steps and methods used to de-identify or aggregate information to protect the confidentiality of the individuals. Contractor shall, at the request of the State, provide the State with a document that lists the steps and methods the Contractor shall use to de-identify the information.
 - (f) Any aggregate or de-identified data that is not properly de-identified or aggregated and is transferred to a third party without the controls of this Section X for Subcontractors or publically released will be considered an Incident, misuse of PII, or unauthorized disclosure of PII.

G. Incident

1. If Contractor becomes aware of an Incident, misuse of PII, or unauthorized disclosure involving any PII, it shall notify the CDE and OIS within one (1) calendar day and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, if any.
2. Unless Contractor can establish that Contractor or any of its Subcontractors is not the cause or source of the Incident, Contractor shall be responsible for the cost of notifying each person whose personal information may have been compromised by the Incident.
3. Contractor shall determine the cause of an Incident and produce a remediation plan to reduce the risk of incurring a similar type of breach in the future. Contractor shall present its analysis and remediation plan to the State within ten (10) calendar days of notifying the State of an Incident. The State reserves the right to adjust this plan, in its sole discretion. If Contractor cannot produce its analysis and plan within the allotted time, the State, in its sole discretion, may perform such analysis and produce a remediation plan, and Contractor shall reimburse the State for the reasonable costs thereof.

4. Disclosure of PII by Contractor or any Subcontractor for any reason may be cause for legal action by third parties against Contractor, the State, or their respective agents. Contractor shall indemnify, save, and hold harmless the State, its employees, and agents against any and all claims, damages, liability, and court awards including costs, expenses, and attorney fees incurred as a result of any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees pursuant to this Section X. Notwithstanding any other provision of this Contract, Contractor shall be liable to the State for all direct, consequential and incidental damages arising from an Incident caused by Contractor or its Subcontractors.
5. In the event of an Incident, Contractor shall provide the State or its designated representatives with access seven (7) days a week, twenty-four (24) hours a day, for the purpose of evaluating, mitigating or resolving the Incident.

H. Disallowed Activities

A Contractor that uses, creates or acquires PII shall not knowingly engage in any of the following activities:

1. Contractor shall not collect, use or share PII for any purpose not specifically authorized by the Contract. Contractor may use PII for a purpose not strictly authorized by the Contract only with the written consent of the State and with the written consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.
2. Contractor shall not use PII in a manner or disclose PII to any third party that is materially inconsistent with the Contractor's privacy policy, except as stated in subsection 3, below, of this Article X, Section I.
3. Contractor may use PII in a manner that is inconsistent with Contractor's privacy policy without violating the terms of this Contract provided that the use does not involve selling or using PII for Targeted Advertising or creating a personal profile of the student, and the use is for one or more of the following purposes:
 - a. To ensure legal or regulatory compliance or to take precautions against liability.
 - b. To respond or to participate in the judicial process.
 - c. To protect the safety of users or others on Contractor's website, online service, online application, or mobile application.
 - d. To investigate a matter related to public safety.

If Contractor uses or discloses PII in accordance with this Section I.3., Contractor shall notify the State within two calendar days of the use or disclosure of the PII.

4. Contractor shall not sell PII, except that this prohibition does not apply to the purchase, merger, or other type of acquisition of the Contractor, or any assets of the Contractor, by another entity, so long as the successor entity continues to be subject to the provisions of this Contract.

5. Contractor shall not use or share PII with any party for the purposes of Targeted Advertising to students.
6. Contractor shall not use PII to create a personal profile of a student other than for supporting the purposes authorized by the State or with the consent of the student (provided that the student is over the age of 18) or the student's parent or legal guardian.

I. Data Security

1. Contractor shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality and integrity of PII. At a minimum, the information security program shall include the requirements listed in this Section J – Data Security. In addition to these requirements, Contractor shall review, on a semi-annual basis, all OIS policies and procedures which OIS has promulgated pursuant to C.R.S. Sections 24-37.5-401 through 406 and 8 C.C.R. Section 1501-5 and posted at <http://oit.state.co.us/ois>, to ensure compliance with the standards and guidelines published therein. All PII received from CDE shall be considered part of the High data security category and Contractor shall comply with all requirements in OIS policies and procedures required for data categorized as High. Contractor shall cooperate, and shall cause its Subcontractors to cooperate, with the performance of security audit and penetration tests by OIS or its designee. In the event of conflicts or inconsistencies between this Section X Confidential Information and OIS policies and procedures, such conflicts or inconsistencies shall be resolved by giving priority to this Section X. Confidential Information.
2. Contractor shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Contract. Contractor shall take full responsibility for the security of all PII in its possession, and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof. Contractor shall provide for the security of such PII, in a form acceptable to the State, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.
3. Contractor shall provide the State or its designated representatives with access, subject to Contractor's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of PII, maintaining State systems, and evaluating physical and logical security control effectiveness.
4. Contractor shall perform, in a form reasonably acceptable to the State, current background checks on all of its respective employees and agents performing services or having access to PII provided under this Contract. The background checks must include, but are not limited to the following areas: County, State, National and Federal Criminal Records and a Sex Offender Registry Search. A background check performed within thirty (30) calendar days prior to the date such employee or agent begins performance or obtains access to PII shall be deemed to be current.
5. Contractor shall have strong access controls in place.

6. Workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended.
7. Contractor shall protect all PII with a complex password. Contractor shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Contractor shall periodically change passwords and shall ensure passwords are not reused. Contractor shall have password locks for laptops and mobile devices.
8. Contractor shall disable and/or immediately delete unused and terminated user accounts. Contractor shall periodically assess account inactivity for potential stale accounts.
9. Contractor shall not share PII on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.
10. Contractor shall implement annual intrusion penetration/vulnerability testing.
11. Contractor shall encrypt PII at rest on central computing systems. Contractor shall also encrypt any backup, backup media, removable media, tape or other copies. In addition, Contractor shall fully encrypt disks and storage for all laptops and mobile devices.
12. Contractor shall provide annual, mandatory security awareness and PII handling training for all of its employees/independent contractors handling PII pursuant to this Contract.
13. Contractor shall install and maintain on computers accessing or processing PII appropriate endpoint security anti-virus and anti-malware software. Contractor shall ensure all Contractor's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.
14. Contractor shall use a secure method such as Secure File Transfer Protocol (SFTP) or comparable method to transmit PII. Contractor shall never send PII via email or transport PII on removable media.
15. Contractor shall have physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.
16. Contractor's devices used to copy or scan hard copies of PII must have encrypted storage. Contractor shall scrub storage devices when equipment is retired. Hard copies containing PII are discouraged and must be physically secured, not left unattended, and physically Destroyed.
17. Contractor shall protect PII stored in cloud based systems in the same manner as local PII. Use of free cloud based services is prohibited. Contractor shall use secondary encryption to protect PII in cloud storage. Cloud environments, when employed by Contractor, must be fully documented by Contractor and open to CDE inspection and verification. Access to Contractor's cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

J. Transparency Requirements

1. No later than thirty (30) calendar days after the signing of this Contract, Contractor shall provide the State with information detailing the purpose and the scope of the Contract, the types of PII that Contractor holds under this Contract, and the uses of PII under this Contract.
2. Contractor shall facilitate access to and correction of any factually inaccurate student PII in response to a request from a local education provider or from the State.
3. Contractor acknowledges that the State will post this Contract to the State's website.
4. Contractor shall provide transparency to parents, school districts and the public about its collection and use of PII including posting the following information on its public website:
 - a. Contact information for an individual within Contractor's organization that can provide information on or answer questions related to the use of PII by Contractor.
 - b. An explanation of how the PII will be shared with Subcontractors or disclosed to any third party.
 - c. The types of PII Contractor collects, generates, or uses. This information must include all PII that is collected regardless of whether it is initially collected or ultimately held individually or in the aggregate.
 - d. An explanation of the PII, an explanation of how the PII is used, and the learning purpose for which the PII is collected and used.

Contractor shall update this information on its website as necessary to maintain accuracy. The Contractor acknowledges that the State will post this information on its public website.

K. Exclusions:

This Section X does not:

1. Impose a duty on a provider of an interactive computer service, as defined in 47 U.S.C Sec. 230, to review or enforce compliance with this Contract.
2. Impede the ability of a student to download, export, or otherwise save or maintain his or her own PII or documents.
3. Limit internet service providers from providing internet connectivity to public schools or to students and their families.
4. Prohibit a Contractor from marketing educational products directly to parents so long as the marketing does not result from the use of PII obtained by the Contractor as a result of providing its services under this Contract.
5. Impose a duty on a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this Contract on that software or those applications.

L. This Section X does not prohibit Contractor's use of PII to:

1. Use adaptive learning or design personalized or customized education.
2. Maintain, develop, support, improve, or troubleshoot a Contractor's website, online service, online application, or mobile application.
3. Provide recommendations for school, education, or employment purposes, provided Contractor does not receive any payment or other consideration from a third party to make or support the recommendation.
4. Respond to a student's request for information or feedback provided Contractor does not receive any payment or other consideration from a third party for the information or feedback.
5. Identify, for a student, institutions of higher education or scholarship providers that are seeking students who meet specific criteria, only if Contractor has obtained the written consent of the student or the student's parent or legal guardian. Contractor may use PII for this purpose regardless of whether the institutions of higher education or scholarship providers provide payment or other consideration to the Contractor.
6. In accordance with the terms of this Contract, produce and distribute, free or for payment or other consideration, student class photos and yearbooks only to the State, students, parents or individuals authorized by parents.
7. Provide for the student, only with the express written consent of the student or the student's parent or legal guardian given in response to clear and conspicuous notice, access to employment opportunities, educational scholarships or financial aid, or postsecondary education opportunities, regardless of whether the Contractor receives payment or other consideration from one or more third parties in exchange for the PII. This exception applies only to Contractors that provide nationally recognized assessments that postsecondary institutions of higher education use in making admissions decisions.

7. START DATE

This Amendment shall take effect on its Effective Date.

8. ORDER OF PRECEDENCE

Except for the Special Provisions, in the event of any conflict, inconsistency, variance, or contradiction between the provisions of this Amendment and any of the provisions of the Contract, the provisions of this Amendment shall in all respects supersede, govern, and control. The most recent version of the Special Provisions incorporated into the Contract or any amendment shall always control other provisions in the Contract or any amendments.

9. AVAILABLE FUNDS

Financial obligations of the state payable after the current fiscal year are contingent upon funds for that purpose being appropriated, budgeted, or otherwise made available to the Department by the federal government, state government and/or grantor.

THE PARTIES HERETO HAVE EXECUTED THIS AMENDMENT

Persons signing for Contractor hereby swear and affirm that they are authorized to act on Contractor's behalf and acknowledge that the State is relying on their representations to that effect.

CONTRACTOR

STATE OF COLORADO

Augenblick, Palaich and Associates, Inc.
Augenblick, Palaich and Associates, Inc.
By: Dale DeGerare
Name of Authorized Individual

John W. Hickenlooper, GOVERNOR
Colorado Department of Education
Katy Anthes, Ph.D., Interim Commissioner
Katy Anthes

Title: Vice President
Official title of Authorized Individual

By: Katy Anthes, Ph.D., Interim Commissioner
Date: 8/16/16

Dale DeGerare
*Signature

ALL CONTRACTS REQUIRE APPROVAL by the STATE CONTROLLER

CRS §24-30-202 requires the State Controller to approve all State Contracts. This Contract is not valid until signed and dated below by the State Controller or delegate. Contractor is not authorized to begin performance until such time. If Contractor begins performing prior thereto, the State of Colorado is not obligated to pay Contractor for such performance or for any goods and/or services provided hereunder.

STATE CONTROLLER
Robert Jaros, CPA, MBA, JD

By: [Signature]
Dave Grier, CPA, CDE Controller

Date: 8-16-2016