CONTRACT AMENDMENT NUMBER 4

VI. PARTIES

This Amendment to the above-referenced Original Contract (hereinafter called the Contract) is entered into by and between ThomasKelly Software Associates, LP, 1 Sugar Creek Center Boulevard, Suite 410, Sugar Land, Texas 77478 (hereinafter called Contractor), and the State of Colorado (hereinafter called the State) acting by and through the Colorado Department of Education (hereinafter called CDE), 201 East Colfax, Denver, Colorado 80203.

VII. 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 State 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.

VIII. FACTUAL RECITALS

The Parties entered into the Contract to implement a state-wide data collection and management system in a web-enabled format for the 21st Century Community Learning Centers (21st CCLC) grant program and automate the annual reporting process to the United States Department of Education (USDOE).

IX. CONSIDERATION-COLORADO SPECIAL PROVISIONS

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. The Parties agree to replacing the Colorado Special Provisions with the most recent version (if such have been updated since the Contract and any modification thereto were effective) as part consideration for this Amendment.

X. 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.

XI. MODIFICATIONS

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

A. Paragraph IV. shall be amended by adding the following definitions:

"Covered Information" means Personally Identifiable Information (PII) and Student Data in any media or format that is created or provided by the State, a school district, a local education agency, a student, or the student's parent or legal guardian to a Contractor in the course of the student's, parent's or legal guardian's use of the Contractor's web site, service or application for public school purposes; or is gathered by a Contractor from any source and contains student PII or Student Data.

"Deliverable" means the outcome to be achieved or output to be provided, in the form of a tangible or intangible object that is produced as a result of Contractor's Work that is intended to be delivered to the State by Contractor. Examples of Deliverables include, but are not limited to, report(s), document(s), server upgrade(s), software license(s), and may be composed of multiple smaller deliverables.

"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 State 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.

"Personally Identifiable Information (PII) Data" means information about an individual collected by the State or any other governmental entity that could reasonably be used to identify such individual as defined in CRS § 24-72-501(2) and includes, but is not limited to, any combination of (i) first and last name, (ii) first name or first initial and last name, (iii) residence or other physical address, (iv) electronic mail address, (v) telephone number, (vi) birth date, (vii) credit card information, (viii) social security number, (ix) driver's license number, (x) identification card number, or (xi) any other information that identifies an individual personally.

"State Confidential Information" means all information, data, records, and documentary materials which are of a sensitive nature and belong to the State regardless of physical form or characteristics, including but not limited to any non-public State records, sensitive State data, protected State data, State personnel records, PII, FTI, PCI, 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 State Records.

"Student Data" means data that is collected and stored by CDE at the individual student level and is included in a student's educational record and includes State-administered assessment results, including participation information, courses taken and completed, credits earned and other transcript information; course grades and grade point average; grade level and expected graduation year; degree, diploma credential attainment or other school exit information; attendance and mobility information between and within Colorado school districts; special education data and special education discipline reports limited to object information that is sufficient to produce the federal Title IV annual incident report; student gender, race, and ethnicity; and program participation information required by state or federal law.

"State Information" means the combination of State Confidential Information and State Records.

"State Records" means all information, data, records, and documentary materials which are not sensitive and belong to the State regardless of physical form or characteristics, including but not limited to any public State records, non-sensitive State data, and other information or data concerning individuals that is not deemed confidential but nevertheless belongs to the State, which has been communicated, furnished or disclosed by the State to Contractor which (i) is subject to disclosure pursuant to the Colorado Open Records Act, C.R.S. Sections 24-72-200.1, et seq.; (ii) is already known to Contractor without restrictions at the time of its disclosure by Contractor; (iii) is or subsequently becomes publicly available without breach of any obligation owed by Contractor to the State; (iv) is disclosed to Contractor, without confidentiality obligations, by a third party who has the right to disclose such information; or (v) was independently developed without reliance on any State Confidential Information. Notwithstanding the foregoing, State Records shall not include State Confidential Information.

"Subcontractor" means any third party engaged by Contractor to aid in performance of Contractor's obligations.

"Summary or De-identified Data" means data on public school students that has all identifiers enumerated in the definitions of PII and Student Data removed.

"Work" means the tasks and activities Contractor is required to perform to fulfill its obligations under this Contract, including the performance of the Services and delivery of the Goods.

"Work Product" means the tangible or intangible results of Contractor's Work, including, but not limited to, software, research, reports, studies, data, photographs, negatives or other finished or unfinished documents, drawings, models, surveys, maps, materials, or work product of any type, including drafts.

B. Paragraph V.A. shall be amended to extend the performance period through December 31, 2016.

C. Paragraph VI.F.1 shall be deleted and replaced with the following:

1. Contractor shall make the system for the 2015-2016 school year available to all Users continuously through December 31, 2016 without any breaks in service.

D. Paragraph Vl.M.5. shall be deleted and replaced with the following:

Contractor shall host the 2015-2016 system through December 31, 2016. For 2016-2017, the system will be set up prior to summer 2016 based on a date to be specified by CDE. CDE Users and Subgrantees will have read only access to data and the ability to save or print reports for the 2015-2016 system.

E. Paragraph Vl.P.I. shall be deleted and replaced with the following:

Contractor shall maintain the data collected under this Contract for the duration of the Contract. CDE Users will have read only access to the 2015-2016 system through December 31, 2016, with the ability to save or print reports.

F. Paragraph VII.C. shall be amended by adding the following new paragraph:

11. Payment in the amount of $2,966 to cover the cost of the privacy insurance required under paragraph XIII.B.8. for calendar year 2016.

G. Paragraph VII.D. shall be amended to increase the maximum amount payable by $8,000 for future customization.

H. Paragraph VII.D. shall be amended by adding a new paragraph VII.D.2. as follows:

Contractor shall directly invoice 21st CCLC Subgrantees and Subgrantees shall pay for the license fee in the amount of $750.00 per site for the period beginning January 1, 2016 and ending December 31, 2016, up to a maximum of $87,750 for 117 sites.

I. Paragraph X. shall be deleted and replaced with the following new Paragraph X.:

X. CONFIDENTIAL INFORMATION-STATE RECORDS

Contractor shall comply with and shall cause each of its Subcontractors and any other party performing Work under this Contract to comply with the provisions of this Section if it becomes privy to State Information in connection with its performance.

A. Confidentiality

Contractor shall comply with all laws and regulations concerning confidentiality of State Confidential Information. Any request or demand by a third party for State Information in the possession of Contractor shall be immediately forwarded to the State's principal representative.

B. Notification

Contractor shall provide its agents, employees, Subcontractors, and assigns who may come into contact with State Information with a written explanation of the confidentiality requirements herein, to which they are subject, before permitting them to access such State Information.

C. Use, Security, and Retention

State Information of any kind shall be stored, processed, or transferred only in or to facilities located within the United States, and shall not be distributed or sold to any third party, retained in any files or otherwise, or used by Contractor or its agents in any way, except as authorized by this Contract, by law, or approved in writing by the State. Contractor shall provide and maintain a secure environment that ensures confidentiality of all State Confidential Information wherever located. Neither Contractor nor its Subcontractors shall have any rights to use or access any CDE or other State agency data or information, except with the prior approval of the State.

D. Protection

Contractor is responsible for the protection and security of all State Information provided to it by the State. If Contractor provides physical or logical storage, processing or transmission of, or retains, stores, or is given, State Information, Contractor shall, and shall cause its Subcontractors to, (i) 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; (ii) maintain network, system, and application security, which includes, but is not limited to, network firewalls, intrusion detection (host and network), and annual security testing; (iii) comply with State and federal regulations and guidelines related to overall security, confidentiality, integrity, availability, and auditing; (iv) ensure that security is not compromised by unauthorized access to computers, program, software, databases, or other electronic environments; and (v) shall promptly report all Incidents to a representative of CDE. Contractor shall provide the State with access, subject to Contractor's reasonable access security requirements, seven (7) days a week, twenty-four (24) hours a day, for the purpose of inspecting and monitoring access and use of State Information, maintaining State systems, and evaluating physical and logical security control effectiveness.

E. Compliance

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. Contractor shall cooperate, and shall cause its Subcontractors to cooperate, with the performance of security audit and penetration tests by OIS or its designee.

F. Delivery and Support

The State, in its sole discretion, may securely deliver State Information directly to the facility where such data is used to perform the Work. State Information is not to be maintained or forwarded to or from any other facility or location except for the authorized and approved purposes of backup and disaster recovery purposes.

G. Incident Notice

If Contractor becomes aware of an Incident involving any State Information, it shall notify the State immediately and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, if any. 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.

H. Incident Remediation

Contractor shall be responsible for determining the cause of an Incident, and for producing 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) 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.

I. Incident Liability

Disclosure of State Information 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 consequential and incident damages arising from an Incident caused by Contractor or its Subcontractors.

J. End-of-Agreement Data Handling

Upon request by the State made before or within sixty (60) days after the effective date of termination of the Contract, Contractor will 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 State Information, schema and transformation definitions, or delimited text files with documented, detailed schema definitions along with attachments in its native format. The Parties agree that on the termination of the provision of data processing services, Contractor shall, at the choice of the State, return all State Information provided by the State to Contractor, and the copies thereof, to the State, or Contractor shall destroy all such State Information and certify to the State that it has done so. If legislation imposed upon Contractor prevents it from returning or destroying all or part of the State Information provided by the State to Contractor, Contractor warrants that it will guarantee the confidentiality of all State Information provided by the State to Contractor and will not actively process such data anymore.

K. Disposition of Data

The State retains the right to use the established operational services to access and retrieve State Information stored on Contractor's infrastructure at its sole discretion. Contractor and Subcontractor warrant that upon request of the State or of the supervisory authority, Contractor will submit its data processing facilities for an audit of the measures referred to in Section X.D. The State reserves all right, title, and interest, including all intellectual property and proprietary rights, in and to system data, State Information, and all related data and content.

L. Safeguarding PII Data

If Contractor or any of its Subcontractors will or may receive PII Data under this Contract, Contractor shall provide for the security of such PII Data, 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, and audits. Contractor shall take full responsibility for the security of all PII Data in its possession or in the possession of its Subcontractors, and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof.

M. Data Security Assurances

1. Strong access control must be in place. All data must be at a minimum protected with a complex password, Contractor workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended. Contractor passwords must be confidential and sharing of passwords is prohibited, must not be written down or stored in an insecure location, and periodically changed and not reused or a reasonable time period.

2. Unused and terminated Contractor user accounts must be disabled and/or deleted immediately; account inactivity must be periodically assessed for potential stale accounts.

3. Care must be exercised in inadvertently sharing data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.

4. Systems must be in place for logging and monitoring Contractor access and use of data.

5. Contractor laptop/mobile device password locks and full disk/storage encryption are required.

6. Data at rest on central computing systems must be encrypted; any backup, backup media, removable media, tape or other copies must also be encrypted, and not used to transport data.

7. Mandatory annual Security awareness training on how to handle PII is required.

8. Appropriate endpoint security anti-virus and anti-malware software must be installed and maintained on servers accessing or processing PII.

9. Transmitting data must occur via a secure method such as Secure File Transfer Protocol (SFTP) or comparable and never sent via email or transported on removable media.

10. Physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.

11. After prescribed use is concluded, data disposal policies must apply for cleaning up all data. This includes secure scrubbing and securely overwriting data from storage, or physically destroying the storage media.

12. Contractor's Devices used to copy or scan hard copies of data must have encrypted storage and have storage devices appropriately scrubbed when equipment is retired. Hard copy containing PPI is discouraged and must be physically secured, not left unattended, and physically destroyed.

13. All Contractor data processing servers must be regularly scanned and have all security patches applied in a timely manner.

N. Transparency Requirements

A Contractor that operates an internet website, an on-line service, including cloud computing services, an on-line application or a mobile application that uses, creates or acquires Covered Information shall not knowingly engage in any of the following activities with respect to its web site, service or application:

1. Engage in targeted advertising of students on the Contractor's web site, service or application, or target advertising on any other web site, service or application when the targeting of the advertising is based upon any information, including Covered Information and persistent unique identifiers, that the Contractor has acquired because of the student's or parent's use of that Contractor's web site, service or application.

2. Use Covered Information, including persistent unique identifiers, created or gathered by the Contractor's web site, service or application, to amass a profile about a public school student, except in furtherance of a public school purpose as determined by the State.

3. Sell Covered Information, including PII to any third party.

4. Disclose Covered Information to any party unless the disclosure is:

   a. Reasonably necessary in furtherance of a public school purpose of the web site, service or application and the recipient of the Covered Information contractually agrees to comply with the requirements herein and to not further disclose the Covered Information,

   b. Required by state or federal law,

   c. Necessary to respond to or participate in a judicial or administrative proceeding,

   d. To protect the safety of users or security of the Contractor's website, service or application, or

   e. To the extent required by law, to provide Covered Information to law enforcement agencies or for an investigation of a matter of public safety.

5. Contractor may not gather or use Covered Information from any source unless it has demonstrated a specific legitimate educational purpose for doing so and the use has been expressly authorized by the Department in the Contract.

6. Contractor must agree to delete Student Data at the request of a School District or Local Educational Agency.

7. Contractor acknowledges that the State will post this Contract to the Department's website and post a privacy score based on the Department's determination of the Contractor's privacy and security protections for Covered Information, with such criteria to include whether Contractor has signed the Student Privacy Pledge, whether Contractor has agreed to all of the Privacy and Security protections in the Department's Policy for Privacy and Security in Third Party Contracts, and the number of complaints received by the Department concerning Contractor's collection or use of Covered Information.

8. Contractor agrees to provide transparency to parents, school districts and the public about its collection and use of Covered Information including:

   a. Post on Contractor's website contact information for the Contractor or Subcontractor that collects or generates Covered Information,

   b. Post on the Contractor's website the types of Covered Information that is collected or generated by the Contractor, its Subcontractors or disclosed to a third party and how the Contractor shares and uses the Covered Information,

   c. Post on the Contractor's website the educational purpose(s) for which the Covered Information is used,

   d. Post on the Contractor's website its policies and procedures regarding retention and disposal of Covered Information,

   e. Upon request, provide CDE with information about the specific data elements that are collected or generated by the Contractor, the Contractor's security policies and any other data that is merged with Covered Information that it collects or generates,

   f. Provide notice on its website to the public before making changes to its privacy policies,

   g. Respond to the Department when an interested party reports an alleged violation of privacy or security laws or the provisions of this Contract, and

O. Exhibit A-3 shall be deleted and replaced with Exhibit A-4, attached hereto and incorporated herein by reference.

XII. START DATE

This Amendment shall take effect on the later of its Effective Date or February 20, 2016.

XIII. 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.

XIV. 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.

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

ThomasKelly Software Associates, LP

By: JEFFREY THOMAS
Name of Authorized Individual

Title: PRESIDENT
Official Title of Authorized Individual

Jeff Thomas
*Signature

STATE OF COLORADO

John W. Hickenlooper, GOVERNOR

Colorado Department of Education
Rich Crandall, CPA, MBA, SNS,
Commissioner

By: Rich Crandall, CPA, MBA, SNS,
Commissioner

Date: 2/17/16

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: _____
Dave Grier, CPA
CDE Controller

Date: 2-19-2016

EXHIBIT A - 4

EZREPORTS SYSTEM IMPLEMENTATION PLAN

1. Contractor shall create a master roster report showing all students and including each student's daily afterschool class schedule and transportation routing using the attached sample.

2. Contractor shall implement the system for Colorado and make it available to all users within 30 days of the effective date of this contract for the 2015 – 2016 school year.

3. CDE, the State Level User, shall enter all grant directors and set their privileges in EZReports.

4. CDE shall set up the State level Assessments in EZReports.

5. An explanation of TKSA EZReports user levels is included herein as a part of this contract:

6. EZReports is a hierarchical user database system. EZReports has separate interfaces for the following three users:

a) **State User** is able to setup and manage all grantees/LEA in the system including defining user privileges for program directors. The state level user is able to setup system wide parameters and can monitor each program or even each site by drilling down to their level. Users at this level have the ability to run system-wide reports and can generate 21st CCLC PPICS (GPR and APR) reports for all 21st CCLC funded programs/sites. The PPICS reports are generated in excel format and can be sent to Learning Points for uploading them in PPICS system without individual program directors having to manually enter all the information.

b) **Program Director** can setup and manage all sites including defining the user privileges for the Site Coordinators. The Program Director can monitor the activities and attendance data for all sites. Several Reports can be generated in real time at the Program Director's discretion.

c) **Site Coordinators** can setup activities, register students, print completed registration forms, enroll and de-enroll students in activities/sessions, generate weekly rosters, enter attendance and print various reports. They can monitor attendance and performance of each student and submit monthly attendance to the Program Director. EZReports enables Site Coordinators to spend less time administering & reporting data and more time focusing on site activities.