Colorado Department of Education
Original Contract Management System Number 63534
Contract Management System Number 92413
CORE 2015-0125

CONTRACT AMENDMENT NUMBER 5

I. PARTIES

This Amendment to the above-referenced Original Contract (hereinafter called the Contract) is entered into by and between SimplyDigi.com, Inc., P.O. Box 90157, Albuquerque, New Mexico 87199-0157 (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.

II. 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.

III. FACTUAL RECITALS

The Parties entered into the Contract to provide a secure web-based workforce registry and course management system to be utilized by early childhood professionals in Colorado. The purpose of this Amendment is to add deliverables, add funding for the new deliverables, to add the ability to use extension amendments, and to update the privacy and security language to comply with 22-16-101 *et. al.*, C.R.S.

IV. 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.

V. 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.

VI. MODIFICATIONS

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

A. Section IV. Definitions, the definition of "Confidential Information" is deleted as it is now redefined in Section XI, Confidential Information.

B. Section V. Term and Early Termination, Subsection C., Extension Amendments, is hereby added to allow extension amendments as published in Request for Proposal NCRS1407035FRCX, Early Childhood Professional Development Information System, as follows:

C. Extension Amendments

The State may require continued performance for a period of one (1) year or less at the same rates and same terms specified in the Contract, unless modified by the extension amendment. Such extension shall be made by contract amendment. An extension amendment is not effective until approved and signed by the Colorado State Controller or an authorized designee. The extended contract shall be considered to include this renewal provision. In no event shall the total duration of this Contract, including any extension amendments under this clause, exceed beyond September 30, 2018, unless the State receives approval from the State Purchasing Director or delegate.

C. The Deliverables and Payment table in Paragraph VIII, shall be amended by adding the following new deliverables to be completed by December 31, 2016:

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
Editor Settings – Credential Group Editor 3.1.1 • 6371 – 3.1.1.1. Revise Labels in Credential Group Editor	All items below to be delivered by December 31, 2016.	$225.00
• 6372 – 3.1.1.2. Allow credential submissions for any level and a specific level		$478.13
• 6373 – 3.1.1.3. Remove existing		

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
properties that are not needed in Credential Group Editor		$225.00
• 6374 – 3.1.1.4. Provide method for configurable drop-down list of reasons not approved		$225.00
Editor Settings		
• 6375 – 3.1.2. Remove unneeded properties for Credential Editor		$225.00
• 6307 – 3.1.3. Professional Development Assessment Editor (previously billed)		$0
• 6376 – 3.1.4. Revise individual Professional Development Plan Rules as described in specifications		$900.00
Configure Credential Award Criteria Provide ability for administrator to configure the following criteria:		
• 6377 – 3.2.1. General Credential Criteria Properties		$590.63
• 6378 – 3.2.2. Criterion: Another Credential / Level		$759.38
• 6379 – 3.2.3. Criterion: Completion of a Specific Course		$506.25
• 6380 – 3.2.4. Criterion: Completion of		

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
Courses in a Specified Course Group		$759.38
• 6381 – 3.2.5. Criterion: Completion of a Self-Assessment for a Specific Competency Group		$759.38
• 6382 – 3.2.6. Criterion: Active IPDP		$506.25
• 6383 – 3.2.7. Criterion: Inclusion of a Specific Goal in the IPDP		$759.38
• 6384 – 3.2.8. Criterion: Document Upload		$590.63
• 6385 – 3.2.9. Criterion: Reference Form Completion		$675.00
• 6386 – 3.2.10. Criterion: Link to a Report		$928.13
• 6387 – 3.2.11. Criterion: Link to Experience Documentation Worksheet		$506.25
• 6388 – 3.2.12. Criterion: Link to Users & Org > User Management page		$506.25
• 6389 – 3.2.13. Criterion: Link to Mange Content > Instructor Profiles Page		$506.25

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
Review and Approve a Manual Credential • 6390 – 3.3.1. Provide dynamic display for Credential Submission List • 6391 – 3.3.2. Provide Administrator Submission Checklist to allow check-off of items as well as add administrator comments		 $900.00 $1,912.50
Criterion Status Provide system to display criterion statuses for each of the following: • 6392 – 3.3.3.1 Criterion: Another Credential / Level • 6393 – 3.3.3.2. Criterion: Completion of a Specific Course • 6394 – 3.3.3.3 Criterion: Completion of Courses in a Specified Course Group • 6395 – 3.3.3.4. Criterion: Completion of a Self-Assessment for a Specific Competency Group • 6396 – 3.3.3.5. Criterion: Active IPDP • 6397 – 3.3.3.6. Criterion: Inclusion of a Specific Goal in the IPDP		 $365.63 $450.00 $618.75 $365.63 $365.63

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
• 6398 – 3.3.3.7. Criterion: Document Upload • 6399 – 3.3.3.8. Criterion: Reference Form Completion • 6400 – 3.3.3.9. Criterion: Link to a Report • 6401 – 3.3.3.10. Criterion: Link to Experience Documentation Worksheet • 6402 – 3.3.3.11. Criterion: Link to Users & Orgs > User Management page • 6403 – 3.3.3.12. Criterion: Link to Manage Content > Instructor Profiles		$703.13 $365.63 $365.63 $365.63 $365.63 $450.00 $365.63
Overall Comments • 6404 – 3.3.4. Provide textbox for administrator Overall Comments		$225.00
Buttons • 6405 – 3.3.5. Provide three Buttons at the bottom of the submission page for administrator: Approve, Cancel, Not		$534.38

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
Approved		
Submission Checklist • 6406 – 3.3.6. Provide Submission Checklist Data Retention Rules as described in specifications		$225.00
Initiate a Manual Credential Application • 6407 – 4.1.1. Modify the existing points-based credential user interface as described in specifications • 6408 – 4.1.2. Add manual credentials that are available in the system		$225.00 $393.75
Apply, Renew, or Upgrade Credential Revise User Interface to following three functions as described in specifications: • 6409 – 4.2.1. Apply • 6410 – 4.2.2. Renew • 6411 – 4.2.3. Upgrade		$759.38 $928.13 $759.38
Complete all Criteria for Submission Based on identification and requirements of credential selected, provide the following interfaces to user in credential submission: • 6412 – 4.3.1. Criterion: Another Credential / Level • 6413 – 4.3.2. Criterion: Completion of		$365.63

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
a Specific Course		$506.25
• 6414 – 4.3.3. Criterion: Completion of Courses in a Specified Course Group		$590.63
• 6415 – 4.3.4. Criterion: Completion of a Self-Assessment for a Specific Competency Group		$225.00
• 6416 – 4.3.5. Criterion: Active IPDP		$225.00
• 6417 – 4.3.6. Criterion: Inclusion of a Specific Goal in the IIPDP		$675.00
• 6418 – 4.3.7. Criterion: Document Upload		$365.63
• 6419 – 4.3.8. Criterion: Reference Form Completion		$1,096.88
• 6420 – 4.3.9. Criterion: Link to a Report		$225.00
• 6421 – 4.3.10 – Criterion: Link to Experience Documentation Worksheet		$309.38
• 6422 – 4.3.11. Criterion: Link to User & Orgs > User Management page (previously billed)		$0
• 6423 – 4.3.12. Criterion: Link to		

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
Manage Content > Instructor Profiles page		$225.00
Submit Revise User Interface to reflect specifications provided for the following: • 6424 – 4.4. Submit the Credential Application		$225.00
Other Enhancements Needed • 6425 – 4.5.1. Provide a method to keep user self-assessment results for differing competency sets separate while providing a method for all results to feed into the Users: "My Learning Professional Development Plan" • 6426 – 4.5.2. Provide a method to save documents uploaded to User Document Portfolio and make this portfolio accessible to the individual user		$928.13 $2,925.00
Enhancements to Points-Based Credentials • 6427 – 5.1. Change "Reject" and "Rejected" Labels to "Not Approved," change "Reason for Rejection" to "Reason Not Approved" • 6428 – 5.2. Provide a Way for User to View the Reason Not Approved • 6429 – 5.3. Change "Diploma/Degree" Label to "Degree" • 6430 – 5.4. Enhance "Years		$590.63 $450.00 $225.00

Contract Deliverables	Estimated Timeline	Cost (not to exceed)
Experience" Status to reflect either "verified" or "self-reported" • 6431 – 5.5. Revise "Years Experience" Points Calculation as described in specifications		$309.38 $675.00
Total		**$33,778.27**

D. Paragraph VIII.A. shall be amended by increasing the maximum amount payable under the Contract by $33,778.27 for a total contract maximum amount payable of $745,570.34.

E. Section XI. Confidential Information-State Records, in order to reflect and comply with 22-16-101 *et. al.*, C.R.S., is hereby deleted in its entirety and replaced with the following Section XI, Confidential Information:

XI. 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. "Data" includes Student Personally Identifiable Information and Educator Data.

3. "Destroy" means to remove Data 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 Data is permanently irretrievable in the Contractor's and Subcontractor's normal course of business.

4. "Educator Data" includes, but is not limited to, the educator's name; any unique identifier, including social security number; and other information that, alone or in combination, is linked or linkable to a specific educator.

5. "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, Educator Data, 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.

6. "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 or Educator Data and shall not include information required to be disclosed pursuant to the Colorado Open Records Act, CRS §24-72-101, et seq.

7. "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.

   Student Personally Identifiable Information also includes 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; date of birth, full name, gender, race, and ethnicity; and program participation information required by state or federal law.

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

9. "Targeted Advertising" means selecting and sending advertisements to an individual based on information obtained or inferred over time from the individual's online behavior, use of applications, or Data. Targeted Advertising does not include advertising to an individual at an online location based on the individual's current visit to that location or in response to the individual's request for information or feedback and is without the collection and retention of an individual'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, Data, and all related data and content.

2. Contractor shall comply with all laws and regulations concerning confidentiality of State Confidential Information and Data including, but not limited to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g; 34 C.F.R. Part 99 and the Student Data Transparency and Security Act, C.R.S. Section 22-16-101 et. seq. Contractor shall immediately forward to the State's principal representative any request or demand from a third party for State Confidential Information or Data 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 XI 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 Data 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 XI.

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 Data, 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 Data 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 Data that Subcontractor(s) holds under the Contract between the Contractor and Subcontractor(s).

5. Contractor shall not maintain or forward Data 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 XI.

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 Data 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 Data, 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 Data 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 Data and State Confidential Information is Destroyed.

4. The State retains the right to use the established operational services to access and retrieve Data and State Confidential Information stored on Contractor's infrastructure at its sole discretion.

F. Use

1. The Contractor shall not use or share Data 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 Data, Contractor shall store, process, and transfer Data only in or to facilities located within the United States.

3. During the term of this Contract, if the State requests the destruction of Data 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. Contractor can retain a student's PII provided that:

   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 Data without complying with the requirements of this Section XI for Subcontractors, Contractor must de-identify or aggregate the Data 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. Data 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 Data 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 individual.

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 XI for Subcontractors or publically released will be considered an Incident, misuse of Data, or unauthorized disclosure of Data.

G. Incident

1. If Contractor becomes aware of an Incident, misuse of Data, or unauthorized disclosure involving any Data, 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 Data 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 XI. 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 Data shall not knowingly engage in any of the following activities:

1. Contractor shall not collect, use or share Data for any purpose not specifically authorized by the Purchase Order. Contractor may use Data for a purpose not strictly authorized by the Purchase Order only with the written consent of the State and, for uses of PII not authorized by the Purchase Order, 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 Data in a manner or disclose Data 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 H.

3. Contractor may use Data in a manner that is inconsistent with Contractor's privacy policy without violating the terms of this Purchase Order provided that the use does not involve selling or using Data for Targeted Advertising or creating a personal profile of the student or educator, 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 Data in accordance with this Section H.3., Contractor shall notify the State within two calendar days of the use or disclosure of the Data.

4. Contractor shall not sell Data, 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 Data with any party for the purposes of Targeted Advertising to students or educators.

6. Contractor shall not use Data to create a personal profile of a student or educator other than for supporting the purposes authorized by the State or, for uses of PII, 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 Data. At a minimum, the information security program shall include the requirements listed in this Section I – 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 Data 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 XI Confidential Information and OIS policies and procedures, such conflicts or inconsistencies shall be resolved by giving priority to this Section XI. 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 Data 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 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, 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 Data, 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 Data 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 Data 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 Data 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 Data 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 Data 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 Data handling training for all of its employees/independent contractors handling Data pursuant to this Contract.

13. Contractor shall install and maintain on computers accessing or processing Data 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 Data. Contractor shall never send Data via email or transport Data on removable media.

15. Contractor shall have physical security in buildings housing Data, along with controlled physical access to buildings and/or data centers.

16. Contractor's devices used to copy or scan hard copies of Data must have encrypted storage. Contractor shall scrub storage devices when equipment is retired. Hard copies containing Data are discouraged and must be physically secured, not left unattended, and physically Destroyed.

17. Contractor shall protect Data stored in cloud based systems in the same manner as local Data. Use of free cloud based services is prohibited. Contractor shall use secondary encryption to protect Data 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.

18. Contractor shall propose detailed, standardized security procedures that CDE shall review and approve. Approved security procedures shall be included in the Annual Work Plan. The security procedures will:

    a. Include a NIST Special Publication 800-18, or equivalent, compliant system security plan.

    b. Define a secure architecture that protects processing, storing, and reporting environments from network-based attacks.

    c. Ensure that electronic files and data are developed, used, and maintained in a secure manner to protect the confidentiality of all personally identifiable information ("PII")

    d. Utilize encryption to ensure security of all director/supervisor/school information entered through all online programs.

19. PDIS shall be a fully secured with a SSL site which meets governmental and SOC 3 compliance.

20. The PDIS shall operate in a class 7 datacenter, directly connected to the internet, with full environmental protection including at a minimum, triplicate levels of; physical, auxiliary power, full Sonnet Ring network protection, unlimited bandwidth capacity, mirrored and balanced servers, data backup and fire suppression.

21. PDIS data shall be maintained in its own virtual environment to provide a firewall between data sources.

22. Backups shall be maintained at a daily, weekly, monthly, and annual level including any nonvolatile backups held off site in vaulted, password protected files and environmentally conditioned storage.

J. Transparency Requirements

1. Contractor acknowledges that the State will post this Contract to the State's website.

2. If Contractor collects, stores or accesses PII, Contractor must comply with the following requirements for transparency:

   a. 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.

   b. 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.

   c. 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 XI 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 XI 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.

XII. START DATE

This Amendment shall take effect on the later of its Effective Date.

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

SimplyDigi.com, Inc.

By: _____
Name of Authorized Individual

Title: CEO
Official title of Authorized Individual

_____
*Signature

STATE OF COLORADO

John W. Hickenlooper, GOVERNOR

Colorado Department of Education
Katy Anthes, Ph.D., Interim Commissioner

_____
By: Katy Anthes, Ph.D., Interim Commissioner

Date: 8/31/16

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: 9-1-2016