CAPITAL REGION BOCES

Approved: 2-11-21

Sourcewell Stretch Agreement (Contract #081419#CDW)
between CDW Government LLC and Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services

This Sourcewell Stretch Agreement ("Agreement") entered into on April 1, 2021 ("Effective Date") by and between CDW Government LLC ("CDW•G" or "Seller") located at 230 N. Milwaukee Ave, Vernon Hills, IL 60061 and Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services ("Customer"), having a place of business at 900 Watervliet-Shaker Road, NY 12205 with a mailing address located at 900 Watervliet-Shaker Road, NY 12205.

The Agreement is as follows:

1. Term; Termination. The term of the Agreement shall commence as of the Effective Date and continue in full force and effect until October 30, 2023, which is the expiration date of Sourcewell Contract #081419#CDW. Should the term of Sourcewell Contract #081419#CDW be extended beyond October 30, 2023, this Agreement shall also be extended to remain coterminous.

Either party may terminate this Agreement without cause upon thirty (30) days prior written notice.

Either party may terminate this Agreement for cause if the other party fails to cure a material default in the time period specified herein. Any material default must be specifically identified in a written notice of termination. After written notice, the notified party will have thirty (30) days to remedy its performance, except that it will only have ten (10) days to remedy any monetary default. Failure to remedy any material default within the applicable time period provided for herein will give cause for immediate termination, unless such default is incapable of being cured within the time period in which case the defaulting party will not be in breach (except for Customer's payment obligations) if it used its reasonable efforts to cure the default.

2. Customer Member. Subject to credit approval and Sourcewell membership confirmation by Seller, and the execution of a mutually agreeable Participation Agreement, a Member may enter into a transaction hereunder. Customer, as set forth above, will not be liable for the performance of the obligations of the Members, including without limitation payment. Customer shall make the terms of this Agreement available to Members. For purposes of this Agreement, the term "Members" means entities that are members of the Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services as set forth in **Exhibit A**, attached hereto and incorporated by reference.

3. Sample Statement of Work. Subject to the terms and conditions of a mutually agreed to Participation Agreement, Seller may perform Services at the Customer's request for Customer or a Member as described in a Statement of Work or SOW(meaning a document in electronic or written form that is signed and delivered by each of the parties for the performance of Services as the same may be amended or modified from time to time by the parties and that incorporates the terms and conditions of this Participation Agreement), which shall substantially take the form of **Exhibit B**, which is incorporated herein. Each SOW constitutes a separate agreement with respect to the Services performed thereunder. In the event of an addition to or a conflict between any term or condition of the SOW and the terms and conditions of this Agreement, the terms and conditions of this Agreement will control, except as expressly amended for an individual SOW by specific reference to the amended provision.

4. Customer Modifications or Additions to the Sourcewell Contract #081419#CDW. Modifications or additions apply only to purchases made by the Customer and its Members.

Customer must check one of the boxes below.

[_____] No changes to the terms and conditions of the Sourcewell Contract #081419#CDW are required.

[_____] The following changes are modifying or supplementing the Sourcewell Contract #081419#CDW terms and conditions:

5. Balance of Terms. Other than the items specifically contemplated herein, the balance of the terms of sale shall be consistent with the Sourcewell Contract #081419#CDW.

In WITNESS WHEREOF, the parties have executed and delivered this Agreement as a document under seal as of the Effective Date.

CDW Government LLC

By: Anup Sreedharan
(Authorized signature)

Anup Sreedharan
Printed Name

Title: Manager, Program Management

Date: Apr 28, 2021

Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services

By: Nancy E delPrado
(Authorized Signature)

Nancy E. delPrado
Printed Name

Title: President, Board of Education

Date: 2-12-21

Exhibit A – Customer Members
Dated _____
to the Sourcewell Stretch Agreement
between CDW Government LLC ("CDW•G")
and the Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services ("Customer")

- **Capital Region BOCES**
- City School District of Albany
- Berne-Knox-Westerlo Central Schools
- Bethlehem Central Schools
- Burnt Hills-Ballston Lake Central Schools
- Cobleskill-Richmondville Central Schools
- Cohoes City Schools
- Duanesburg Central Schools
- Green Island Union Free School
- Guilderland Central Schools
- Menands School
- Middleburgh Central Schools
- Mohonasen Central Schools
- Niskayuna Central Schools
- North Colonie Central Schools
- Ravena-Coeymans-Selkirk Central Schools
- Schalmont Central Schools
- Schenectady City Schools
- Schoharie Central Schools
- Scotia-Glenville Central Schools
- Sharon Springs Central School
- Shenendehowa Central Schools
- South Colonie Central Schools
- Voorheesville Central Schools
- Watervliet City Schools

- **Champlain Valley Educational Services**
- AuSable Valley Central School District
- Beekmantown Central School District
- Chazy Central Rural School District
- Crown Point Central School District
- Elizabethtown-Lewis Central School District
- Keene Central School District
- Moriah Central School District
- Northeastern Clinton Central School District
- Northern Adirondack Central School District
- Peru Central School District
- Plattsburgh City School District
- Putnam Central School District
- Saranac Central School District
- Schroon Lake Central School District
- Ticonderoga Central School
- Westport Central School
- Willsboro Central School

- **Franklin-Essex-Hamilton BOCES**
- Brushton-Moira Central School District
- Chateaugay Central School
- Lake Placid Central School District
- Long Lake Central School District
- Malone Central School District
- Raquette Lake Union Free District
- St. Regis Falls Central School
- Salmon River Central School District
- Saranac Lake Central School District
- Tupper Lake Central School District

- **Hamilton-Fulton-Montgomery BOCES**
- Greater Amsterdam School District
- Broadalbin-Perth Central School District
- Canajoharie Central School District
- Edinburg Common School District
- Fonda-Fultonville Central School District
- Fort Plain Central School District
- Gloversville Enlarged School District
- Greater Johnstown School District
- Lake Pleasant Central School District
- Mayfeld Central School District
- Northville Central School District
- Oppenheim-Ephratah St Johnsville Central School District
- Wells Central School District
- Wheelerville Union Free School District

- **Questar III**
- Averill Park Central School District
- Berkshire Union Free School District
- Berlin Central School District
- Brunswick (Brittonkill) Central School District
- Cairo-Durham Central School District
- Catskill Central School District
- Chatham Central School District
- Coxsackie-Athens Central School District
- East Greenbush Central School District
- Germantown Central School District
- Greenville Central School District
- Hoosic Valley Central School District
- Hoosick Falls Central School District
- Hudson City School District
- Ichabod Crane Central School District
- Lansingburgh Central School District
- New Lebanon Central School District
- North Greenbush Common
- Rensselaer City School District
- Schodack Central School District
- Taconic Hills Central School District
- Troy City School District
- Wynantskill Union Free School District

- **St. Lawrence-Lewis BOCES**
- Brasher Falls Central School District
- Canton Central School District
- Clifton- Fine Central School District
- Colton-Pierrepont Central School District
- Edward Knox Central School District
- Gouverneur Central School District
- Hammond Central School
- Harrisville Central School District
- Herman Dekalb Central School District
- Heuvelton Central School District
- Lisbon Central School District
- Madrid Waddington Central School District
- Massena Central School District
- Morristown Central School District
- Norwood Norfork Central School District
- Ogdensburg City School District
- Parishville Hopkinville Central School District
- Potsdam Central School District

- **Washington-Saratoga-Warren-Hamilton-Essex BOCES**
- Abraham Wing Common School
- Argyle Central School
- Ballston Spa Central School
- Bolton Central School
- Cambridge Central School
- Corinth Central School
- Fort Ann Central School
- Fort Edward Union Free School
- Galway Central School
- Glens Falls City School
- Granville Central School
- Greenwich Central School
- Hadley-Luzerne Central School
- Hartford Central School
- Hudson Falls Central School
- Indian Lake Central School
- Johnsburg Central School
- Lake George Central School
- Mechanicville City School
- Minerva Central School
- Newcomb Central School
- North Warren Central School
- Queensbury Union Free School
- Salem Central School
- Saratoga Springs City Schools
- Schuylerville Central School
- South Glens Falls Central School
- Stillwater Central School
- Warrensburg Central School
- Waterford-Halfmoon Union Free School
- Whitehall Central School

EXHIBIT B

STATEMENT OF WORK

Project Name:	[Project Name]	**Seller Representative:** [Seller Name] [Seller Phone] [Seller e-mail]
Customer Name:	[Customer Name]	
CDW Affiliate:	[CDW Affiliate determined by Customer #]	
Subcontractor:	[Partner Name]	**Solution Architect:** [Solution Architect Name], [Solution Architect Name 2]
SOW Created Date:	[SOW Created Date]	
Version:	[File Version]	**Drafted By** [Services Contract Specialist Name]

This statement of work ("**Statement of Work**" or "**SOW**") is made and entered into on the last date that this SOW is fully executed as set forth below ("**SOW Effective Date**") by and between the undersigned, [CDW Affiliate] ("**Provider**," and "**Seller**,") and [Customer Name] ("**Customer**," and "**Client**,").

GOVERNING AGREEMENT

This SOW shall be governed by that certain [Governing Agreement Name] between [CDW Affiliate] and [Customer Name], dated [Governing Agreement Date] (the "**Agreement**"). If there is a conflict between this SOW and the Agreement, then the Agreement will control, except as expressly amended in this SOW by specific reference to the Agreement. References in the Agreement to a SOW or a Work Order apply to this SOW.

PROJECT SCOPE

SERVICE DESCRIPTION

GENERAL RESPONSIBILITIES AND ASSUMPTIONS

- Customer is responsible for providing all access that is reasonably necessary to assist and accommodate Seller's performance of the Services.
- Customer will provide in advance and in writing, and Seller will follow, all applicable Customer's facility's safety and security rules and procedures.
- Customer is responsible for security at all Customer-Designated Locations; Seller is not responsible for lost or stolen equipment, other than solely as a result of Seller's gross negligence and willful misconduct.
- This SOW can be terminated by either party without cause upon at least fourteen (14) days' advance written notice.

CONTACT PERSONS

Each Party will appoint a person to act as that Party's point of contact ("**Contact Person**") as the time for performance nears and will communicate that person's name and information to the other Party's Contact Person.

Customer Contact Person is authorized to approve materials and Services provided by Seller, and Seller may rely on the decisions and approvals made by the Customer Contact Person (except that Seller understands that Customer may require a different person to sign any Change Orders amending this SOW). The Customer Contact Person will manage all communications with Seller, and when Services are performed at a Customer-Designated Location, the Customer Contact Person will be present or available. The Parties' Contact Persons shall be authorized to approve changes in personnel and associated rates for Services under this SOW.

CHANGE MANAGEMENT

This SOW may be modified or amended only in a writing signed by both Customer and Seller, generally in the form provided by Seller ("**Change Order**"). Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

In the event of a conflict between the terms and conditions set forth in a fully executed Change Order and those set forth in this SOW or a prior fully executed Change Order, the terms and conditions of the most recent fully executed Change Order shall prevail.

PROJECT SCHEDULING

Customer and Seller, who will jointly manage this project, will together develop timelines for an anticipated schedule ("**Anticipated Schedule**") based on Seller's project management methodology. Any dates, deadlines, timelines or schedules contained in the Anticipated Schedule, in this SOW or otherwise, are estimates only, and the Parties will not rely on them for purposes other than initial planning.

TOTAL FEES

CUSTOMER DESIGNATED LOCATIONS

Seller will provide Services benefiting the locations specified on the attached Schedule A ("**Customer-Designated Locations**").

PROJECT SPECIFIC TERMS

EDUCATION LAW 2-D

IF APPLICABLE, SELLER SHALL COMPLY WITH THE REQUIREMENTS SET FORTH IN NEW YORK STATE EDUCATION LAW SECTION 2-D AND SHALL COMPLY WITH THE PROVISIONS SET FORTH IN SCHEDULE "B", ATTACHED HERETO AND INCORPORATED BY REFERENCE.

Education Law 2-D ☐ is applicable to the Services ☐ is not applicable to the Services

INSURANCE

Seller shall comply with the insurance requirements set forth in Schedule "C," attached hereto and incorporated by reference.

SIGNATURES

In acknowledgement that the parties below have read and understood this Statement of Work and agree to be bound by it, each party has caused this Statement of Work to be signed and transferred by its respective authorized representative.

This SOW and any Change Order may be signed in separate counterparts, each of which shall be deemed an original and all of which together will be deemed to be one original. Electronic signatures on this SOW or on any Change Order (or copies of signatures sent via electronic means) are the equivalent of handwritten signatures.

[CDW Affiliate Name]	**[Customer Name]**
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date: _____	Date: _____
Mailing Address:	**Mailing Address:**
[Affiliate Address line 1]	Street:_____
[Affiliate Address line 2]	City/ST/ZIP: _____

SCHEDULE A

CUSTOMER-DESIGNATED LOCATIONS

Seller will provide Services benefiting the following locations ("**Customer-Designated Locations**").

Location(s)

Schedule "B"

This Schedule "B" is part and parcel to the SOW dated _____ by and between CDW Government LLC ("Seller") and Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services ("Customer").

This agreement ("Agreement") made and entered into effective as of the _____, 202_ ("Effective Date") is by and between, CDW Government LLC., (hereinafter "Contractor") and the Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services (hereinafter "CUSTOMER"). Contractor and CUSTOMER shall be collectively referred to as "the Parties,"

WHEREAS, Contractor will receive student data and/or teacher or principal data in possession of CUSTOMER and/or its officers, employees, agents, and students, and may also receive student data and/or teacher or principal data of educational agencies within New York State that enter into contracts for services with CUSTOMER for the use of data services and Contractor's services;

WHEREAS, Contractor desires to have access to this information in order to fulfill its contractual obligations to its customers;

WHEREAS, CUSTOMER desires to use Contractor's services in order to aid in providing services to its customers; and

WHEREAS, in entering into this Agreement, the Parties seek to address compliance with N.Y. Education Law § 2- d and 8 N.Y.C.R.R. § 121.1, *et seq*.;

NOW, THEREFORE, in consideration of the foregoing and the mutual covenants herein contained, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

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

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

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

c. "Disclose" or "Disclosure" means to permit access to, or the release, transfer, or other communication of Personally Identifiable Information (as defined below) by any means, including oral, written, or electronic, whether intended or unintended.

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

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

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

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

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

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

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

k. "Student data" means Personally Identifiable Information from the student records of an educational agency. For purposes of this agreement, "student data" includes information made accessible to Contractor by CUSTOMER, CUSTOMER officers, CUSTOMER employees, CUSTOMER agents, CUSTOMER students, and/or the officers, employees, agents, and/or students of

educational agencies with whom CUSTOMER contracts.

l. "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this agreement, "student data" includes information made accessible to Contractor by CUSTOMER, CUSTOMER officers, CUSTOMER employees, CUSTOMER agents, CUSTOMER students, and/or the officers, employees, agents, and/or students of educational agencies that contract with CUSTOMER in order to access Contractor's services.

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

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

a. Applicable state and federal laws that protect the confidentiality of Personally Identifiable Information;

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

c. CUSTOMER policies, which can be accessed on the CUSTOMER website at: TBD.

3. Contractor will not use subcontractors in fulfilling its responsibilities to CUSTOMER, its employees or agents, and/or educational agencies which contract with CUSTOMER for the provision of Contractor's services.

4. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers or employees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees who have access to Personally Identifiable Information will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to that data.

CDW's Global Privacy Training Program

CDW's Global Privacy Policy is incorporated into CDW's Road to Success, which is acknowledged by employees at the time of hire and on a regular basis post-hire. Employees also receive training on CDW's Global Privacy Policy at the time of hire and on a regular basis post-hire. For employees whose duties require either handling data that is subject to data protection laws or whose duties include some compliance activity related to those laws, targeted and specialized training is conducted. Failure to abide by CDW's Global Privacy Policy or to adhere to established protocol can lead to disciplinary action.

Road to Success Completion Training Criteria Includes the Following:

- Understanding personal data
- Key principles of data privacy
- Importance of stopping and thinking before accessing or sharing personal data
    - Personal data defined as follows: SSN, Customer ID, Email addresses, cell phone numbers, birthdates, photos, job title, IP address, credit card numbers, government ID number
- Protecting Data
- Review of Global Data Privacy Policy
    - Transparency
    - Restrict unnecessary collection, use and access
    - Respect a person's wishes
- Privacy Statement
- Collection of Data
- Accessing Data
- Respecting Data
- Sharing Data
- Working with Data

CDW's Global Privacy Program

As a multinational technology company, CDW places a high value on respecting the data privacy of its customers, partners and employees. To that end, CDW operates a global privacy training program that works on a centralized model with implementation expected from a range of front-line employees. The CDW Data Privacy Policy Training is required for all employees. Employees must pass a web-based exam as evidence of completion and comprehension.

1.0 Structure and Oversight

1.1 Central Responsibility

Responsibility for designing and maintaining the global privacy program falls under CDW's Ethics and Compliance Office. The Ethics and Compliance Office is part of CDW's Legal Department and reports to CDW's General Counsel, who is accountable to

CDW's Board of Directors and Audit Committee. Ethics and Compliance acts as the central hub for privacy compliance across all CDW entities and locations.

1.2 Coordinated Cross-Functional Compliance

As the central hub for privacy compliance, Ethics and Compliance relies on all employees to execute the day-to-day operations of its global corporate privacy program. Ethics and Compliance also works closely with those functions that are most critical to the privacy program, including Information Security, Information Technology, and Human Resources. Employees in certain functions have been trained and tasked with specific privacy compliance responsibilities, including executing workflows related to data subject access rights, data privacy impact assessments, and privacy by design.

2.0 Elements

CDW complies with applicable data protection laws worldwide through a number of mechanisms.

2.1 Contracts

Where applicable law requires certain contractual terms to be in place, CDW maintains appropriate contract templates which are regularly reviewed for compliance with those laws. When existing contracts are reviewed or renewed on a routine basis, existing contract terms are revised where necessary to comply with applicable law. In some circumstances when dictated by applicable law, as when the General Data Protection Regulation was approaching its date of enforcement, a large-scale contract amendment project may be implemented across various affected groups, including customers and suppliers.

2.2 Operations

2.2.1 Registrations and DPO

CDW Limited is registered with the United Kingdom's Information Commissioner's Office, with the registration number Z1427546 as a data processor. CDW as an organization has a global data protection officer registered in a number of jurisdictions, including the European Union and Singapore.

2.2.2 Notices

CDW's privacy notice is available here. The same privacy notice is also available on all other CDW websites, including websites for the United Kingdom and Canada. CDW also maintains a privacy notice specifically for job applicants, which is available . Certain geographies for which CDW maintains separate external websites also maintain separate stand-alone cookie policies and procedures, which are available on the relevant websites.

2.2.3 Data Inventories

As required by EU data protection law, CDW maintains a written record of processing activity related to its processing of EU personal data. This record is reviewed on both a routine and ad hoc basis, such as when new technology is deployed.

2.2.4 Individual Access Rights

CDW has documented internal procedures to ensure appropriate response to enquiries from employees, independent contractors and customers or other external data subjects.

2.2.5 Privacy-by-Design and Data Privacy Impact Assessments

CDW has integrated checkpoints for privacy design controls into its information technology change management processes in both the United States and the European Union. CDW also maintains an internal procedure governing when and in what circumstances privacy reviews or data privacy impact assessments shall be conducted.

2.2.6 Security Incidents

Responsibility for data security incidents rests mainly with CDW's Information Security team. Security incidents are handled pursuant to a written policy and procedure based on industry standards and in accordance with applicable law. There are multiple methods to report suspected security incidents; those methods are routinely publicized to employees.

2.2.7 Complaints and Investigations

CDW has a dedicated email account for the submission of questions, access requests or complaints regarding data protection. The account is publicly listed on CDW's website and monitored by the data protection officer and the Legal Department's Ethics and Compliance Office. In addition, CDW maintains a third-party service to allow the reporting of privacy issues by external parties; this third-party service is linked in CDW's privacy notice. Employees may also report issues or ask questions anonymously through CDW's ethics hotline, which is widely publicized to employees.

2.2.8 International Data Transfer

CDW employs multiple legal mechanisms when transferring data across borders. For customer data, CDW is self-certified under the EU-US Privacy Shield

2.2.9 Third Party Risk Management Third party risk management is primarily the responsibility of the partner management organizations in the United States and the United Kingdom. Privacy controls have been integrated into the processes for review of suppliers in both geographies. Supplier contracts are tailored for compliance with applicable laws.

2.2.10 Routine Program Review The various elements of CDW's privacy program are reviewed both regularly as a matter of course and on an ad hoc basis, such as when there is a change in law. These reviews may take the form of efficacy reviews by Ethics and Compliance, internal audits conducted by CDW's Business Process Assurance department, or external audits.

2.3 Training CDW's Global Privacy Policy is incorporated into CDW's Road to Success, which is acknowledged by employees at the time of hire and on a regular basis post-hire. Employees also receive training on CDW's Global Privacy Policy at the time of hire and on a regular basis post-hire. For employees whose duties require either handling data that is subject to data protection laws or whose duties include some compliance activity related to those laws, targeted and specialized training is conducted. Failure to abide by CDW's Global Privacy Policy or to adhere to established protocol can lead to disciplinary action.

5. The exclusive purpose for which Contractor is being provided access to Personally Identifiable Information is to **assist CUSTOMER with deploying and integrating the hardware and software solution.** Contractor does not monitor or use customer content for any reason other than as part of providing our services.

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

7. Upon expiration or termination of this Agreement without a successor agreement in place, Contractor shall assist CUSTOMER and any educational agencies that contracts with CUSTOMER for the provision of Contractor's services in exporting any and all student data and/or teacher or principal data previously received by Contractor back to CUSTOMER or the educational agency that generated the student data and/or principal data. Contractor shall thereafter securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related

work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data and/or teacher or principal data will be completed within 30 days of the expiration/termination of this Agreement between CUSTOMER and Contractor, and will be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Contractor and/or its subcontractors or assignees will provide a certification to CUSTOMER from an appropriate officer that the requirements of this paragraph have been satisfied in full.

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

9. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States, or a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily be limited to disk encryption, file encryption, firewalls, and password protection.

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

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

b. Not use Personally Identifiable Information, education records/and or student

data for any purpose other than those explicitly authorized in this Agreement;

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

d. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Personally Identifiable Information in its custody;

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

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

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

h. Contractor will cooperate with CUSTOMER, any educational agency that contracts with CUSTOMER for Contractor's services, and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Personally Identifiable Information.

11. In the event of a data security and privacy incident implicating the Personally Identifiable Information of students, teachers, and/or principals of CUSTOMER

or educational agencies which contract with CUSTOMER for the provision of Contractor's services:

a. Contractor has an Incident Response Policy that is established to require the creation and maintenance of a structured Incident Response Plan to guide its response to security events, incidents, and breaches of the security of Contractor's services or corporate IT infrastructure. Contractor's Information Security Overview is attached as Exhibit B and is incorporated by reference.

b. Contractor will notify CUSTOMER, and any educational agency that contracts with CUSTOMER for Contractor's services, of any such incident in accordance with Education Law § 2-d, 8 N.Y.C.R.R. Part 121, and paragraph 11(f), above.

12. This AGREEMENT, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, constitutes the entire understanding of the Parties with respect to the subject matter thereof. The terms of this AGREEMENT, together with the signed Parents Bill of Rights for Data Privacy and the Security and Supplemental Information to Parents Bill or Rights for Data Privacy and Security, shall supersede any conflicting provisions of Contractor's terms of service or privacy policy.

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

14. This AGREEMENT shall be governed by the laws of the State of New York. The Parties hereto agree that exclusive venue for any litigation, action or proceeding arising from or relating to this Agreement shall lie in the state and federal courts located in _____ County, New York, and the Parties expressly waive any right to contest such venue for any reason whatsoever.

In witness of the foregoing, the duly authorized representatives of the Parties have signed this Agreement as of the Effective Date set forth above.

CONTRACTOR CUSTOMER

BY: _____	BY: _____
NAME:	NAME:
TITLE:	TITLE:

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

This Exhibit A is part and parcel to the Data Privacy and Security Agreement dated June 10, 2020 by and between CONTRACTOR ("Contractor") and the Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services ("CUSTOMER").

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

1. A student's Personally Identifiable Information (PII) cannot be sold or released for any commercial or marketing purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record. This right of inspection is consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.

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

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

5. Parents have the right to file complaints with NERIC about possible privacy breaches of student data by NERICs third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints regarding student data breaches should be directed to: Michele Jones, DPO, NERIC, 900 Watervliet Rd, Albany, NY 12205. Phone: 518-862-5300; e-mail: michele.jones@neric.org

6. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email: CPO@mail.nysed.gov.

SUPPLEMENTAL INFORMATION TO PARENTS BILL OR RIGHTS FOR DATA PRIVACY AND SECURITY:

1. The exclusive purpose for which Contractor is being provided access to student data and/or teacher or principal data is to provide application programing interface and data exchange services. Contractor does not monitor or use customer content for any reason other than as part of providing our services.

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

3. Contractor agrees that any of its officers or employees who have access to Personally Identifiable Information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data. More specifically, Contractor has received the required training. Furthermore, Contractor requires all employees to undergo security awareness and privacy training upon hire and yearly thereafter.

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

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

applicable educational agency's Annual Professional Performance Review Plan.

6. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

7. Any student data and/or teacher or principal data possessed by Contractor will be protected using encryption technology while in motion, in its custody and at rest.

ACKNOWLEDGED AND AGREED TO BY:

Signature: _____

Name: _____

Title: _____

Date: _____

NORTH AMERICA

CDW INFORMATION SECURITY OVERVIEW

TABLE OF CONTENTS

1.0 INTRODUCTION

In today's increasingly complex IT environment, companies must protect their information. At CDW, information security is a top priority for all parts of our business. Our comprehensive policies and procedures are designed to safeguard customer information and ensure its confidentiality, integrity and availability.

This document outlines the key foundational principles of CDW's Information Security Program and describes how CDW maintains its commitment to information protection.

2.0 ABOUT CDW

CDW is a leading provider of integrated technology solutions. We help our small, medium and large business, government, education and healthcare customers by delivering critical solutions to their increasingly complex IT needs.

Our broad array of offerings ranges from discrete hardware and software products to integrated IT solutions such as mobility, security, data center optimization, cloud computing, virtualization and collaboration. Regardless of the products or services a customer chooses to purchase from CDW, our goal is to maximize the customer's return on technology investment while striving to meet the highest industry standards for information security.

3.0 CDW'S INFORMATION SECURITY PROGRAM

In order to protect and secure our customers' information, CDW has created a comprehensive Information Security Program, led by our chief information security officer. The goal of our Information Security Program is to protect the confidentiality, integrity and availability of CDW's customer information in accordance with applicable laws, industry standards and other obligations. CDW's policies and procedures for the handling of our customers' information are designed to ensure CDW's information systems are appropriately safeguarded.

CDW communicates the requirements and expectations of the Information Security Program, as well as the consequences for noncompliance (which may include termination, legal action or other responses as appropriate) to all employees, contractors, business partners and anyone else authorized to access customer information on CDW's behalf (collectively referred to as "Authorized Users").

CDW's Information Security Program is supported by periodic risk assessments designed to proactively identify internal and external risks to our information and information systems, and determine if existing controls, policies and procedures are adequate.

4.0 AUTHORIZED USER SECURITY

Screening

CDW requires applicants to undergo background checks as a condition of hiring. These background checks may include one or more of the following, depending on the applicant's location, roles and responsibilities:

- Criminal background check
- SSN/SIN Validation
- Employment history/education verification
- Credit check

Confidentiality Agreements

CDW employees, contractors and temporary employees are required to sign applicable privacy and confidentiality agreements upon hire. These agreements set forth the responsibilities and restrictions for dealing with CDW's and our customers' confidential information.

Information Security Training

CDW takes information security seriously and requires that its Authorized Users understand and follow policies related to internal and customer information protection. All employees are required to attend and complete periodic information security education and awareness training. Depending on the employee's role and access to information, the subject and depth of training may vary.

A key requirement in training is that all CDW employees are instructed to immediately report suspected information security incidents as required by CDW policies.

Termination

CDW has established processes for ensuring that confidential information remains secure when an Authorized User is separated from CDW. We immediately collect all CDW-owned assets such as laptops and other mobile devices from the terminated individual according to our Asset Management Policy and ensure a timely removal of that person's rights to access CDW information systems, networks, premises and customer information.

5.0 INFORMATION CLASSIFICATION

CDW maintains a written Information Classification Policy, which classifies information based on its sensitivity and security needs. These classifications dictate how we process, store, transport and transmit CDW's and our customers' information. In order to protect information, we limit access to and control information as needed per these classifications.

All information classified as Confidential or Highly Confidential under the Information Classification Policy — whether CDW's own information or information maintained by CDW on a customer's behalf — is afforded the protections required for such information under CDW's information security policies and procedures. Any special information handling instructions required by the customer should be specified through customer contract terms and conditions.

6.0 ENCRYPTION AND KEY MANAGEMENT

CDW recognizes that some information requires heightened security. Accordingly, we encrypt certain sensitive information, including information classified as Confidential or Highly Confidential, at rest and/or in transit, as appropriate based on the information classification and CDW's information security policies. CDW uses industry-standard methods of cryptography and maintains detailed key management processes to ensure that keys are securely managed and appropriately protected.

7.0 IT ASSET MANAGEMENT

Our policies address the security of IT assets, including their use and return. In accordance with CDW policy, IT assets are monitored to identify their location, user and disposition at any given time. CDW has also outlined the roles and responsibilities for who manages each asset category, as well as how those assets are managed from distribution to destruction.

8.0 ACCOUNT MANAGEMENT AND ACCESS CONTROL

An important element of information security is controlling access to sensitive information. Access to information and the CDW information systems that house such information is restricted to Authorized Users with a legitimate business need. All Authorized Users are required to authenticate to CDW's information systems using a unique user ID and password that meet industry-standard complexity requirements. Where appropriate for access to environments and systems, multifactor, one-time-use passwords may be used.

For Authorized Users who need remote access to CDW's information systems, our policies require multifactor authentication for remote access.

9.0 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical access to CDW data centers is restricted to a limited number of approved Authorized Users who have a legitimate business need for access. Physical access to the data center does not confer access to information.

To provide additional security, physical access to the data centers is monitored 24/7 with video surveillance, with videos retained in accordance with CDW's Records Retention Schedule. Security guards are present at entrances and CDW has a defined visitor access check-in process for all locations. Escorts are required when accessing data centers.

Our information security policies extend to any facility that stores or processes CDW information (including our customers' information entrusted to CDW), including facilities that CDW does not own or lease. We require these facility service providers to enforce physical and environmental security controls in accordance with CDW's policies and procedures.

10.0 BUSINESS CONTINUITY AND DISASTER RECOVERY

CDW has developed a Business Continuity Plan and corresponding Disaster Recovery Policy and Disaster Recovery Plan. CDW has implemented appropriate disaster recovery strategies, such as high-availability systems, for critical information systems to ensure CDW's information systems recovery capabilities meet business needs, as well as to ensure CDW's ongoing ability to provide solutions and services to its customers.

11.0 BACKUP

CDW backs up its information systems using tape and tapeless solutions implemented for its own infrastructure. CDW's information security policies define the information to be backed up, backup frequency, and backup monitoring requirements. Where applicable and appropriate, backup tapes are stored offsite and tested at least annually to confirm restores can be performed from the backups.

12.0 LOGGING AND MONITORING

CDW configures and retains audit logs and alerts in accordance with internal and external requirements. To accomplish this, CDW identifies and evaluates its information systems and other systems to determine where audit logging and other monitoring controls are needed. CDW's information security policies define the minimum requirements for types of information collected for each audit event. In addition, applicable infrastructure is monitored for availability and performance to help ensure ongoing service delivery to our customers.

13.0 CHANGE MANAGEMENT/SDLC

CDW follows change management and software development lifecycle (SDLC) policies and processes in order to manage change in its information systems and to ensure all changes are developed securely. All changes must be tested and approved by appropriate CDW management. Approved changes are moved into a "live" environment only by Authorized Users.

CDW also maintains the security of its information systems by applying patches on a periodic basis. Patching follows the change management processes.

14.0 INFORMATION SYSTEMS SECURITY

A major goal of our Information Security Program is to defend against security intrusion through a combination of layered prevention technologies and comprehensive security monitoring. Our security infrastructure has been designed according to industry standards for virus protection, firewalls and intrusion-prevention technologies in order to prevent unauthorized access or compromises of CDW's network, systems and servers.

To maintain this level of security, CDW:

- Periodically tests systems to identify/remediate information security issues
- Conducts vulnerability scans
- Uses industry-standard security resources to obtain up-to-date information on security issues across many technologies
- Monitors network connections with intrusion prevention/detection systems
- Bans use of insecure protocols in infrastructure management or transmitting sensitive information
- Configures network and system devices so event logs are maintained in a centralized system
- Requires CDW management approval for any direct connections to our information systems
- Isolates guest wireless networks and unauthenticated connectivity from CDW internal traffic

15.0 INCIDENT MANAGEMENT

Our focus is to protect against and detect unauthorized access or loss of CDW's or its customers' information. If an information security event does occur, CDW has policies and procedures in place to ensure the appropriate personnel are alerted, and to take the necessary steps to remediate the information security event and mitigate any harm. In the event of an information security incident, CDW has a defined incident response plan to appropriately manage, escalate and resolve that incident. The plan defines how and when a response team is created and what its responsibilities are. We also comply with applicable legal and regulatory requirements when determining escalation and customer notification of a breach or significant event. We ensure our procedures meet our internal standards for incident management and annually test our response plan.

16.0 THIRD-PARTY MANAGEMENT

CDW has relationships with third-party providers to deliver services to customers. We contractually require any such third party accessing or processing customer information to ensure the security of that information. The third party's contractual obligations to CDW may cover a range of issues, including adoption of specific security practices, protection of confidential information and adherence to compliance requirements.

17.0 AUDIT AND COMPLIANCE

CDW is a global company that serves clients operating in many different industries. As such, CDW is subject to a range of compliance requirements. CDW complies with various compliance requirements, frameworks and certification standards including but not limited to the following:

- Sarbanes-Oxley Act ("SOX")
- Health Insurance Portability and Accountability Act ("HIPAA")
- Payment Card Industry Data Security Standard ("PCI DSS")
- General Data Protection Regulation ("GDPR")
- Personal Information Protection and Electronic Documents Act ("PIPEDA")
- ISO/IEC 27001 Information Security Standard
- Statement on Standards for Attestation Engagements No. 18 ("SSAE 18")

18.0 RECORDS RETENTION

CDW has a Records Retention Policy and corresponding Records Retention Schedule to define the retention period for various types of records. In accordance with the record disposal requirements included in our Records Retention Schedule, we follow industry standards for secure disposal, whether electronic or paper form. If we are hosting information for a customer, the customer is responsible for defining and enforcing their record retention schedule.

19.0 CDW WEBSITE SECURITY

The following statements refers to CDW.com, CDW.ca, and CDWG.com.

CDW knows that its customers are concerned about the security of online purchases, so our security policies require that our web applications be monitored by multiple technologies, as well as various internal applications. We ensure product information is up to date per manufacturer-provided information, and our inventory systems are designed to reflect accurate counts on all CDW application platforms.

We also track traffic and usage with third-party applications and rigorously monitor web application health. CDW uses operating system tools to evaluate server health and runs cloud-based synthetic tests at predetermined intervals from various locations across North America to ensure availability on the internet.

Finally, CDW maintains active web certificates from an authorized external certificate authority.

20.0 PRIVACY PROGRAM

The CDW Global Privacy Program Overview can be made available upon request.

Schedule “C”

Insurance Requirements

This Schedule “C” is part and parcel to the SOW dated _____ by and between CDW Government LLC (“Seller”) and Albany – Schoharie – Schenectady-Saratoga Board of Cooperative Educational Services (“CUSTOMER”).

1. Notwithstanding any terms, conditions or provisions, in any other writing between the parties, Seller hereby agrees to effectuate the naming of CUSTOMER as an additional insured on the Seller’s insurance policies, with the exception of workers' compensation, NY State disability and professional liability. If the policy is written on a claims-made basis, the retroactive date must precede the date of the contract.

2. The policy naming CUSTOMER as an additional insured shall:
    a. Be an insurance policy from an A.M. Best rated "secured" insurer, authorized to conduct business in New York State; and
    b. State that the Seller’s coverage shall be primary coverage for CUSTOMER, its Board, employees and volunteers.

3. CUSTOMER shall be listed as an additional insured by using endorsement CG 2026 or equivalent. The certificate must state that this endorsement is being used. If another endorsement is used, a copy shall be included with the certificate of insurance. The decision to accept an alternative endorsement rests solely with CUSTOMER.

4. Required Insurance:

    a. Commercial General Liability Insurance
    $1,000,000 per occurrence/ $2,000,000 aggregate.

    b. Workers' Compensation and N.Y.S. Disability
    Statutory Workers' Compensation, Employers' Liability and N.Y.S. Disability Benefits Insurance for all employees.

    c. Professional Errors and Omissions Insurance
    $2,000,000 per occurrence/ $2,000,000 aggregate for the professional acts of Seller performed under the contract for CUSTOMER. If written on a “claims-made” basis, the retroactive date must pre-date the inception of the contract or agreement. Coverage shall remain in effect for two years following the completion of work.

d. Excess Insurance

On a “Follow-Form” basis, with limits of $3,000,000 each occurrence and aggregate.

5. Seller acknowledges that failure to obtain such insurance on behalf of CUSTOMER constitutes a material breach of contract. At the request of Customer, Seller shall provide CUSTOMER with a certificate of insurance, evidencing the above requirements have been met, prior to the commencement of work or use of facilities.