

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -  
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	Summit Consulting Group, Inc. DBA BrightShift Inc.
<b>PII Declaration</b>	<p><b>Does your organization/software collect student personally identifiable information (PII) or staff PII?</b></p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> <li>a. The student’s name;</li> <li>b. The name of the student’s parent or other family members;</li> <li>c. The address of the student or student’s family;</li> <li>d. A personal identifier, such as the student’s social security number, student number, or biometric record;</li> <li>e. Other indirect identifiers, such as the student’s date of birth, place of birth, and Mother’s Maiden Name;</li> </ul> <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> <li>a. Teacher ID</li> <li>b. Name</li> <li>c. Birthdate</li> <li>d. Gender</li> <li>e. Race</li> <li>f. Salary</li> </ul> <p><input type="checkbox"/> <b>IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</b></p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	We deliver certification exams for several programs. This data is used solely to associate the student with a test event so that the certifying body may award a certification certificate to the student. These certificates are then provided by the student to employers for entry-level and more advanced positions. Our system integrates with Clever and ClassLink so any PII is either entered by the student/instructor or is provided through sharing rules set up by the district or school for our use solely for the purpose above through these third-party systems..
<b>Type of PII that Contractor will receive/access</b>	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input checked="" type="checkbox"/> APPR PII</p>

<b>Contract Term</b>	Contract Start Date <u>11/27/2023</u> Contract End Date <u>07/01/2025</u>
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)  <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall:  • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.  • Securely delete and destroy data.
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)  <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other:  Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:  All data resides at Rackspace Managed Hosting (Rackspace). Data is stored encrypted and is transmitted encrypted. Rackspace does not have the encryption key.
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

**CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN**

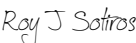
The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	The company Privacy Officer shall be responsible for the implementation of any and all data security and privacy requirements. Additionally, we work very closely with our systems hosting company Rackspace as well as all our certification body partners to ensure all PII is treated in a secure manner.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	All data is encrypted while at rest and while in transit. Additionally, all passwords are SALTED using a random SALT for each password. Encryption keys are stored off-site in a separate facility. No one has access to any PII other than the certification bodies we deliver tests for.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All employees and contractors (currently only 3 and they have been with the company each for over 5 years) receive training on the latest security and privacy requirements. Dual authentication is utilized for all our systems. Since we are all small organization everyone is advised of each data security agreement we sign as well as any internal data security changes in our own policies. Training is provided in an ongoing manner.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All contractors (only 3) have signed contracts and NDAs that address many things including the importance of data security and the damage any breach might inflict on our company, schools, instructors, and students.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice. Such notice will include information about what we have done to protect individuals whose information has been breached. Advice on steps that the person whose information has been breached may take to protect himself or herself. Information about the steps we have
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	We can supply this data in any manner required by the EA but we typically permanently delete the data from our systems upon request. In addition, all PII data is purged from our system every 3 years since our certification bodies typically only award 2-year certifications.
7	Describe your secure destruction practices and how certification will be provided to the EA.	We shall dispose of or delete all Data obtained under the Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to EA or EA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Summit is committed to the security of all data in our system. As such we are a proud member of A4L and have adopted their standard as our own for the security of data as well as plans in the event a breach occurs or a destruction request is provided to us by the EA. We believe our A4L standard aligns perfectly with the EA
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	We and our hosting provider as well as our contractors all work to adhere to a framework that matches NIST CSF. Specifically, we identify our data, risk to our data, data flows, and access control. We protect our data through the implementation of security controls, encryption

## Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: [dpo@wsboces.org](mailto:dpo@wsboces.org). (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Roy J Sotiros
[Title]	President
Date:	11/27/2023

January 13, 2022