Supplemental Information

Pursuant to Education Law § 2-d and § 121.3 of the Regulations of the Commissioner of Education, NYSED is required to post information to its website about its contracts with third-party contractors that will be provided Access to or receive Disclosure of Student Data and/or APPR Data.

1. **Name of Contractor:** Southern Tier Independence Center, Inc. C051315

2. **Description of the exclusive purpose(s) for which the Student Data and/or APPR Data will be used:**

3. **Type(s) of Data that Contractor will be provided:**

   Yes Student Data

   Yes APPR Data

4. **Contract Term:**

   Contract Start Date: 07/01/2024

   Contract End Date: 06/30/2029

5. **Subcontractor use and written agreement requirement:**

   No Contractor will use Subcontractors.

If Contractor plans to use Subcontractors, 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 this contract.

   N/A Contractor agrees to bind its Subcontractors by written agreement.

6. **Data Transition and Secure Destruction**

Yes Contractor agrees that the confidentiality and data security obligations under this DPA will survive the expiration or termination of this contract but shall terminate upon Contractor's certifying, that Contractor and its Subcontractors:

a. Are unable to Access any Information provided pursuant to this contract; and
b. Securely transfer Disclosed Student Data and APPR Data to NYSED, or at NYSED's option and written discretion, a successor contractor in a format agreed to by the Parties**;** and
c. Securely deleted and destroyed Disclosed Student Data and APPR Data.

7. Challenges to Data Accuracy

Yes Contractor agrees that parents, eligible students, teachers, or principals who seek to challenge the accuracy of Student Data or APPR Data will be referred to NYSED and if a correction to data is deemed necessary, NYSED will notify Contractor. Contractor further agrees to facilitate such corrections within 21 days of receiving NYSED's written request.

8. Secure Storage and Data Security

Please indicate where Student Data and/or APPR Data will be stored:

No Using a cloud or infrastructure owned and hosted by a third party.

Yes Using Contractor owned and hosted solution.

No Other:

Please describe how data privacy and security risks will be mitigated in a manner that does not compromise the security of the data:

STIC has policies and procedures in place to protect the confidentiality of Personally Identifiable Information (PII) in the performance of this contract. STIC's policies mandate that access to the PII is restricted solely to staff who need such access to carry out the responsibilities of their job, and that such staff will not release such information to any unauthorized party. Personally Identifiable Information (PII) is stored both in hard copy (paper) format and electronically.

PII that is in paper format is stored in individual consumer files located in the office of the employee providing service to the consumer. The office is locked at all times when not in use by the staff person. Only the staff person providing service to the individual, or his/her supervisor, has access to the information on a regular basis. The PII is also accessed occasionally by STIC's quality Management Specialist for audit and compliance activities. Electronic PII is stored on the computer of the employee providing service to the consumer. The computer is located in the employee's office, which remains locked when not in use.

All employee computers are encrypted and require a user name and password for access. Therefore, only individuals entering a valid user name along with the correct password can access a workstation. Only the employee, his/her supervisor, and STIC's IT Department have access to the password for an employee's computer. All employees are required to shut down their computers when they will be away from them. All offices that contain PII are locked when not in use. All confidential Data stored on computers and within STIC are behind appropriate hardware firewalls.

According to STIC policy, PII that is stored electronically must be backed up each time it is changed. All backed-up information is stored on an encrypted and password protected thumb drive. Only the employee in possession of the thumb drive and STIC's IT Department have the password to access this external drive.

STIC's policies prohibit sending PII in the body of an email, but rather in an encrypted document. All documents transmitted by STIC via email that contain PII are zipped and password protected to ensure that they are encrypted.

9. Encryption requirement

Yes Contractor agrees that Student Data and APPR Data will be encrypted while in motion and at rest.

10. Contractor Certification.

Contractor certifies that Contractor will comply with, and require its Subcontractors to comply with, applicable State and Federal laws, rules, and regulations and NYSED policies.

Contractor's Name **Southern Tier Independence Center, Inc. C051315**