Central Islip Union Free School District Program Information and Data Privacy Third Party Agreement

To be completed **by the vendor** and submitted for all NEW and RENEWAL software/programs prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor. Failure to complete this form in its entirety will significantly delay any/all program purchases.

Software/Program Title:	ACTFL Assessment of Performance toward Proficiency in Languages® (AAPPL)
Publisher:	Language Testing International, Inc.
Contract Pricing	☐ BOCES Contract or Shared Service ☐ NYS Contract Pricing ☐ Federal Contract Pricing ☒ Direct Bid/RFP with Vendor
Account Management	☐ SSO through LDAP/AD/ADFS/AZURE/SAML ☐ SSO through Clever ☒ NO SSO Option ☐ Non SSO Centrally Managed (all Users) ☐ Non-User Based Program/Not Applicable
Platform	☐ Local Install OR Device APP ☐ Local Server/Network ☒ 100% Web-based ☐ Web-Based with Local application/plug-in ☐ Other/Explain:
License Structure:	☐Per-User ☒Per-Student ☐Per-Classroom ☐Per-Teacher ☐Per-Building ☐Districtwide/Unlimited
License Renewal	☐Perpetual (no-renewal) ☐Annual X Single-use
Separate Hosting Fees:	☒NO ☐YES - Annually ☐Other/Explain:

Contractor Initials: JR JR

Adobe Flash	☒Program DOES NOT require Adobe Flash ☐Program REQUIRES Adobe Flash Programs that still require Adobe Flash will not be considered for purchase or utilized
Configuration, Deployment, Initial Roll-Out Support	☐ Full On-Site Support Included in the Proposal/Fee ☒ Remote Support Only ☐ Remote Support Included/On-Site for Additional Fees
Staff Training/Professional Development	☐ Full On-Site Training/Development Included in the Proposal/Fee ☒ Remote/WebEx Training/Development and Support Only ☐ Combined On-Site/WebEx Training included in proposal
SIS-PowerSchool Integrations	☒ Program DOES NOT sync to SIS (PowerSchool) ☐ Program DOES sync to SIS (PowerSchool) ☐ Not Applicable

ALL LINKS MUST BE PROVIDED AND COMPLETED BY THE VENDOR!

Software Title:	ACTFL Assessment of Performance toward Proficiency in Languages® (AAPPL)
Publisher/Developer:	Language Testing International, Inc.
Developer/Vendor Name	Language Testing International, Inc.
Developer/Vendor Mailing Address	580 White Plains Road, Suite 660 Tarrytown, NY 10591
Developer/Vendor Privacy Policy Link:	https://www.languagetesting.com/lti-information/privacy
Developer/Vendor Parent Bill of Rights Link	n/a (Vendor does not interact directly with parents / legal guardians. If a parent / legal guardian contacts the Vendor, Vendor will refer them to the school/district.)

Contractor Initials: JR JR

This Data Privacy Agreement ("DPA") is by and between the Central Islip Union Free School District (herein known as "EA"), an Educational Agency, and the above listed software, app or extension developer (herein known as "Contractor"), collectively, the “Parties”.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor’s security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** 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.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** 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 Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal prekindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** 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.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: 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 Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated below ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("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); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**

   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.

   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.*

*__EA:__ Contractor has attached its standard NY Exhibits C and C.1 to the end of this DPA.

Contractor Initials: JR JR

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

Contractor Initials: JR JR

7. Training.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors 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.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach.

Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor’s investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA’s District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Philip K. Voigt
Director of Instructional Technology
50 Wheeler Rd
Central Islip, NY 11722
Pvoigt@centralislip.k12.ny.us

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its’ Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EXHIBIT A - 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. 65016502 (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 https://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 the EA's Director of Technology at pvoigt@centralislip.k12,ny.us (ii) Complaints may also be submitted to the NYS Education Department at https://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; or by telephone at 518-474-0937.

7. 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.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Contractor Initials: JR JR

EXHIBIT B

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).

Description of the purpose(s) for which Contractor will receive/access PII	Description: Student data are limited to first and last name, school issued ID number (any format), and test scores; LTI receives no contact information for students. Teacher and principal data, including name, email address, and phone number, are used when accounts and subaccounts are created on Contractor's Client Site. ☐ NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☒ Employee PII (See above response.)
Contract Term	Each Contract is valid through the software renewal period or 3 school years in the case of "Free" programs, apps, extensions and pilots.
Data Transition and Secure Destruction	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.
Challenges to Data Accuracy	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.
Encryption	☒ Data will be encrypted while in motion and at rest.

As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breeches or intrusions associated with this program, applications, software or browser extension.

Dec 18, 2023

Signature of Vendor Official Representative

Date

Signature must be an actual signature and cannot be a script font or text. If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.

EXHIBIT C - CONTRACTOR’S DATA PRIVACY AND SECURITY PLAN

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.	By maintaining our current data security and privacy protocols and best practices as described below. All LTI employees undergo a criminal background check prior to being hired and all have received training on federal and New York state laws governing confidentiality of PII. This training is repeated in the form of an annual mandatory refresher course. Additionally, LTI limits the internal access to PII to those individuals who need to see it to perform their job functions. Thus, only a small number of LTI employees (currently 3) have access to PII. As part of its standard best practices regarding data security, • LTI complies with federal, state, and local laws regarding data security and privacy and their implementing regulations. • LTI does not use PII for any purpose other than those explicitly authorized in its contracts. • LTI does not sell or disclose PII for marketing or commercial purposes. • LTI does not disclose PII to any third party: ○ unless required by statute or court order with the provision that the party provides notice of the disclosure to the school, district, department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order. • LTI maintains reasonable administrative, technical, and physical safeguards (e.g., encryption, firewalls, and password protection) to protect the security, confidentiality, and integrity of PII. • LTI uses TLS 1.2 to secure data in motion and 256-bit AES encryption technology or higher to protect data while at rest in its custody from unauthorized disclosure. LTI uses technology, safeguards, and practices that align with the NIST Cybersecurity Framework (Version 1.1). LTI also has various types of security policies and controls in place for data protection, privacy, and information security. LTI has implemented role-based access that limits the information a user has access to and is reviewed at least once every 12 months. LTI also has implemented various types of software and network management tools to alert/deny access to LTI systems.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	LTI employees are assigned roles on a need-to-know basis. PII data stored in databases are AES 256-bit encrypted. LTI's infrastructure & web applications are beyond well architected solutions and firewalls that deny all network traffic except SSL (TLS 1.2). **From the *LTI Access Control Policy*:** LTI will strictly control access to information resources under their direction or ownership. When approving access rights LTI Deputed IT Security Person should consider the following: • Users’ need for access

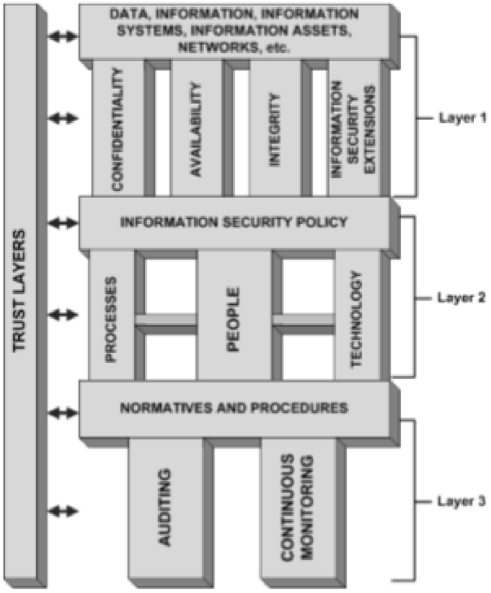
		• Potential conflict with segregation of duties • Any regulatory requirements • Level of access required (read, update, delete) • Period for access. **User Account review Process:** User Account monitoring and management controls provide a gatekeeper function to prevent and detect unauthorized activities that may lead to loss of covered data. These controls allow resource proprietors and resource custodians to control precisely who has access to data and detect inappropriately granted access before data loss events occur. Review of user access and accounts is performed as per chart listed in LTI User account review process document which requires a review at least once every 12 months. **From the *LTI Facility Access Policy*:** Physical access to all restricted facilities shall be documented and managed. All facilities must be physically protected relative to the criticality or importance of the function or purpose of the area managed. Requests for access shall come from the applicable manager in the area where the data/system resides. Access to facilities will be granted only to personnel whose job responsibilities require access. Electronic access control systems shall be used to manage access to controlled spaces and facilities. LTI's door access code will be issued only to LTI employees. The door access code is not, under any circumstance, to be given to any other person, regardless of reason.
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 LTI employees, even those who will not have access to client PII, receive training on federal and New York state laws governing the confidentiality of protected data. This training is repeated in the form of an annual mandatory refresher course. All LTI developers follow secure coding practices, and all development takes into account the most current OWASP guidelines. LTI developers are required to undergo a secure coding training program at least every 12 months. New IT employees must undergo their 1st secure coding training program 6–12 months after their hire date.
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 LTI employees must sign an NDA at the start of employment, which covers and does not permit disclosure of "any information about any customer." LTI sub-contractors must sign a similar NDA.
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.	LTI will promptly notify the EA of any breach or unauthorized release of PII it has received from the EA in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after LTI has discovered or been informed of the breach or unauthorized release. LTI will cooperate with the EA and provide as much information as possible, including but not limited to: • a description of the incident, • the date of the incident, • the date LTI discovered or was informed of the incident, • a description of the PII involved, • an estimate of the number of records affected, • the schools within the district affected, • what LTI has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of PII,

		• and contact information for LTI representatives who can assist affected individuals that may have additional questions.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	EA may download and export all student test result data from the secure LTI Client Site in Excel format.
7	Describe your secure destruction practices and how certification will be provided to the EA.	LTI's Process for Destruction of Client Data 1. If requested by the EA, all student test data may be downloaded from the LTI Client Site in Excel format before destruction. (EA should also request a final certificate of destruction at this time.) 2. After confirmation that the EA's testing account has been paid in full, LTI will initiate a data destruction request. 3. The data are destroyed. 4. The data destruction is internally validated. 5. If requested by the EA before initiation of the data destruction request, a certificate of destruction will be returned to the EA once this process is complete.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	LTI is in compliance with the Contractor responsibilities as stated in the Third-Party Contractor Responsibilities section (pp. 6–7) of **NY State DOE Policy #5676 - Privacy and Security for Student Data and Teacher and Administration Data** found at https://www.p12.nysed.gov/specialed/nyssb/includes/documents/PrivacyandSecurityforStudentTeacherandAdministratorData.pdf. If more information is required, please clarify.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	The LTI Asset Management Policy informs LTI staff about policies regarding Information Technology (IT) Asset Management. The policy establishes and enforces technical and administrative controls to support asset management, both in internal operations and external AWS Infrastructure. LTI's IT Department is charged with the ongoing management of technology assets and the efficient and accountable use of IT Budget to funds these assets represent. An Asset Management policy allows LTI to: 1. Make informed IT planning, procurement, and investment decisions 2. Calculate IT asset value and understand the total cost of ownership of those assets 3. Manage the acquisition, maintenance, and decommissioning of key asset types 4. Prepare to replace assets that are technically at End of Life 5. Prepare to replace assets that are no longer supported by original provider 6. Monitor compliance with IT standards 7. Allocate support resources efficiently and effectively 8. Secure and protect IT assets
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	LTI has established Access Control and Acceptable Use policies for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access. The Access Control Policy helps LTI to implement security best practices regarding logical security, account management, and remote access. All employees and vendors/consultants must be given authorized access to any LTI information resource. The authorization will be granted on an as needed basis by the relevant manager. Access to information resources should be restricted to authorized personnel only to prevent and detect unauthorized access or abuse. To maintain effective information security, it is vital for LTI to ensure that data can only be accessed and processed by authorized personnel. Amazon Web Services (AWS), Hostway, and Nexcess for our hosting facility as well as our local premise datacenter. LTI will review all access to these facilities. Access consists of access to LTI data and software/hardware installation. LTI will strictly control access to information resources under their direction or ownership. When approving access rights, the LTI Deputed IT Security Person should consider the following: • Users' need for access • Potential conflict with segregation of duties • Any regulatory requirements • Level of access required (read, update, delete) • Period for access
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational	The way we assess security is based on a layered architecture with components connected in such a way that everything is part of a puzzle that must be well connected and understood so that information security can be seen as a whole.

Function	Category	Contractor Response
	requirements are understood and inform the management of cybersecurity risk.	The image below illustrates the information security architecture and its layers. Its topics describe each layer in a top-down explanation and its corresponding subtopics, in addition to a brief description of its importance to the puzzle.  DATA, INFORMATION, INFORMATION SYSTEMS, INFORMATION ASSETS, NETWORKS, etc. CONFIDENTIALITY AVAILABILITY INTEGRITY INFORMATION SECURITY EXTENSIONS Layer 1 INFORMATION SECURITY POLICY PROCESSES PEOPLE TECHNOLOGY Layer 2 NORMATIVES AND PROCEDURES AUDITING CONTINUOUS MONITORING Layer 3 TRUST LAYERS
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	As the threat landscape becomes more challenging over time, we continuously monitor activity and usage patterns to determine areas of improvement. Our management team meets periodically to determine mitigation priority items and to plan with our scheduling team.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	The management team evaluates on a periodic basis the threat landscape and our risks and considers how to proceed with due diligence.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	N/A

PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	LTI has implemented an Access Control Policy and a User Accounts Review Process to control access to resources. All employees and vendors/consultants must be given authorized access to any LTI information resource. The authorization will be granted on an as needed basis by the relevant manager. Access to information resources should be restricted to authorized personnel only to prevent and detect unauthorized access or abuse. To maintain effective information security, it is vital for LTI to ensure that data can only be accessed and processed by authorized personnel. Amazon Web Services (AWS), Hostway, and Nexcess for our hosting facility as well as our local premise datacenter. LTI will review all access to these facilities. Access consists of access to the LTI data and software/hardware installation. LTI will strictly control access to information resources under their direction or ownership. When approving access rights, the LTI Deputed IT Security Person should consider the following: • Users' need for access • Potential conflict with segregation of duties • Any regulatory requirements • Level of access required (read, update, delete) • Period for access User Account monitoring and management controls provide a gatekeeper function to prevent and detect unauthorized activities that may lead to loss of covered data. When implemented correctly, these controls allow resource proprietors and resource custodians to control precisely who has access to data and to detect inappropriately granted access before data loss events occur. **Account Management** • Record and monitor significant changes to system user accounts and groups to ensure that access is not granted outside. Significant user account and group changes include: ○ Status changes that enable or disable accounts/groups ○ Account access privilege updates ○ Account creation/deletion ○ Group access privilege updates ○ Group membership updates ○ Group creation/deletion **Account Review** • Review accounts assigned to both users and applications/services as shown in **Chart 1** below (next page). • Validate the continued business need for each active account with the resource and ensure that application/service account credentials will be disabled when no longer needed. • Reconcile existing active accounts with account access requests; any access privileges not approved by the Director of IT should be noted and revoked immediately. • Review account and privilege updates, with special emphasis on administrative privilege updates, for suspicious activities that may signal compromised accounts. Examples of suspicious activities include unauthorized changes to existing administrative accounts and privileges, new administrative accounts/groups created without approval or documentation, etc. • Modifying Access: Access modifications must include a valid authorization. When there is a position change (not including separation), access is immediately reviewed and removed when no longer needed.

- Review of privilege accounts must be carried out in specific to ensure that those are not being used for a regular or daily task by a standard user.

Chart 1

Type	Roles	Review Periodicity
LTI Applications	Functional / Standard	Quarterly
Network components - Servers - Firewalls - Routers - etc.	Privileged Users	Quarterly
Network components - Servers - Firewalls - Routers - etc.	System accounts	Yearly
Cloud Services E.g. Salesforce, Tableau, AWS, DigiCert etc.	Functional / Standard	Quarterly
Cloud Services E.g. Salesforce, Tableau, AWS, DigiCert etc.	Privileged Users	Quarterly

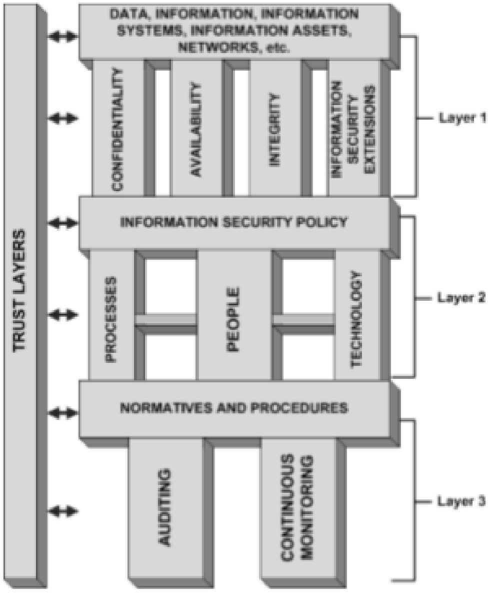
Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

All LTI employees undergo a Data Privacy, protection, and information security training program annually.

All LTI developers shall follow secure coding practices. All development shall be done taking the most current OWASP guidelines into account.

LTI developers will be required to undergo a secure coding training program at least every 12 months.

New employees undergo their 1st secure coding training program 6–12 months after their hire date.

	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	The way we assess security is based on a layered architecture with components connected in such a way that everything is part of a puzzle that must be well connected and understood so that information security can be seen as a whole. The image below illustrates the information security architecture and its layers. Its topics describe each layer in a top-down explanation and its corresponding subtopics, in addition to a brief description of its importance to the puzzle.  DATA, INFORMATION, INFORMATION SYSTEMS, INFORMATION ASSETS, NETWORKS, etc. CONFIDENTIALITY AVAILABILITY INTEGRITY INFORMATION SECURITY EXTENSIONS Layer 1 INFORMATION SECURITY POLICY PROCESSES PEOPLE TECHNOLOGY Layer 2 NORMATIVES AND PROCEDURES AUDITING CONTINUOUS MONITORING Layer 3 TRUST LAYERS
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	LTI has implemented various types of policies and processes: Access Management, User Account Review Process, Data Classification, Logging and Monitoring, SDLC Policy, Change Management, Privileged Account Management, Facility Access Process, etc.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	N/A - AWS
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Our systems and assets are protected through centrally managed security solutions that align with our infosec policies and the goals of management to eliminate or reduce security risks.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Our Security Management infrastructure consists of the following systems and platforms: **Wazuh** for Intrusion Detection, covering real-time security events, integrity monitoring and vulnerability detection; **AWS Guard Duty** for real-time monitoring of the AWS account and networking, **AWS Inspector** for vulnerability scanning and reporting and **AWS Config** for CMDB and compliance. These tools allow proper real-time reporting and classification of existing events and vulnerabilities according to their criticality.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	All systems are monitored and scanned using the platforms detailed in the previous points and rescanned once a patch or update has been implemented, to verify the remediation. Our internal SOC team is in charge tracking each event throughout its lifecycle across the different channels.

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes and procedures are maintained and tested constantly and updated when required.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	In the same way, response processes and procedures are maintained and tested constantly and updated when required.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	When a security event is detected, our SOC team tracks the issue in our internal systems and contacts the appropriate parties within the company to begin the remediation process. The flow is different depending on the criticality of the event.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Analysis is one of the first stages in our incident response plan. It involves assessing the issue, contacting the right parties, and restoring the services back to normal as soon as possible.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Once an event has been detected, we perform corrective activities as needed either to mitigate or fully restore the services.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	After the services are restored, our team performs a root cause analysis focused on identifying preemptive measures to prevent the issue from happening in the future. Actions are tracked and followed up accordingly.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Recovery processes and procedures are maintained and tested constantly and updated when required. This includes activities such as backup integrity checks and disaster recovery testing.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	After each root cause analysis, all computational or human driven processes are reviewed and updated as required. Retrospectives are also carried out as part of our agile approach to management.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and Language Testing Internationals).	In accordance with our processes, when an incident is identified, one of our engineers is assigned the role of "incident commander." This engineer is in charge of making sure the incident response processes are properly executed and following up with all the internal and external parties until the incident is resolved.

2023 data privacy agreement_LTI_for Jay to sign

Final Audit Report 2023-12-18

Created:	2023-12-18
By:	Allen Bernier (abernier@languagetesting.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAszee-sIKz45n6hPHcZTRD7aVcn1tekxV

"2023 data privacy agreement_LTI_for Jay to sign" History

Document created by Allen Bernier (abernier@languagetesting.com)

2023-12-18 - 9:49:05 PM GMT- IP address: 97.91.84.24

Document emailed to Jay Rhyu (jrhyu@languagetesting.com) for signature

2023-12-18 - 9:51:04 PM GMT

Email viewed by Jay Rhyu (jrhyu@languagetesting.com)

2023-12-18 - 11:28:45 PM GMT- IP address: 98.110.64.27

Document e-signed by Jay Rhyu (jrhyu@languagetesting.com)

Signature Date: 2023-12-18 - 11:29:42 PM GMT - Time Source: server- IP address: 98.110.64.27

✓ Agreement completed.

2023-12-18 - 11:29:42 PM GMT