

EXHIBIT A

DATA PRIVACY AND SECURITY TERMS AND CONDITIONS

for the Master Agreement between Orchard Park Central School District (“District”) and Language Testing International, Inc. (“Vendor”) (collectively the “Parties”)

WHEREAS, the District and Vendor are parties to a contract or other written agreement for purposes of providing certain products or services to the District (“Master Agreement”); and

WHEREAS, Education Law §2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) require the Parties to have certain terms and conditions governing the privacy and security of certain data the Vendor will receive pursuant to the Master Agreement; and

WHEREAS, the Parties are desirous to set forth such terms and conditions in this Exhibit to the Master Agreement;

NOW THEREFORE, in consideration of the mutual promises set forth in the Master Agreement, the Parties agree to the following terms and conditions.

A. DEFINITIONS

1. “Student Data” means personally identifiable information from the student records of the District that Vendor receives pursuant to the Master Agreement.
2. “Teacher or Principal Data” means personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under Education Law §§ 3012-c and 3012-d that Vendor receives pursuant to the Master Agreement.
3. “Protected Data” means Student Data and/or Teacher or Principal Data, as defined above.

B. PURPOSE

1. Pursuant to the Master Agreement, the Vendor will receive Protected Data from the District for purposes of providing certain products or services to the District.
2. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with these Terms and Conditions, these Terms and Conditions will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of the products or services that are the subject of the

Master Agreement between the District and Vendor, these Terms and Conditions shall supersede any conflicting terms of the TOS.

C. DATA SHARING AND CONFIDENTIALITY

1. Vendor Acknowledgments

i. Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

ii. Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and will comply with the District's policy on data privacy and security. The District will provide Vendor with a copy of its policy on data privacy and security upon request.

2. Vendor's Data Privacy and Security Plan

i. Vendor will implement all state, federal, and local data privacy and security requirements and such requirements contained within the Master Agreement and these Terms and Conditions including but not limited to the requirements set forth in the Parents' Bill of Rights and the Supplemental Information set forth below, consistent with the District's data privacy and security policy.

ii. Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

iii. Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees or assignees, if applicable, who will have access to Protected Data, prior to receiving access.

iv. If Vendor uses any subcontractor(s), Vendor will require such subcontractor(s) or other authorized persons or entities to whom it may disclose Protected Data to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law, the Master Agreement, and these Terms and Conditions shall apply to the subcontractor.

v. Vendor will follow certain procedures for the return, transition, deletion, and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement as set forth in detail in the Supplemental Information below.

vi. Vendor will manage data privacy and security incidents that implicate Protected Data and will develop and implement plans to identify breaches or unauthorized disclosures. Vendor will provide prompt notification to the District of

any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 3 herein.

3. Notification of Breach or Unauthorized Release

With respect to any breach or unauthorized release of Protected Data, including any breach or unauthorized release of Protected Data by Vendor's assignees or subcontractors, Vendor acknowledges and agrees to the following:

i. Vendor will promptly notify the District of any breach or unauthorized release of Protected Data, in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

ii. Vendor will provide such notification to the District by contacting the Data Protection Officer directly by email at privacy@opschools.org or by calling 716-209-6330.

iii. Vendor will cooperate with the District and provide as much information as possible directly to the Data Protection Officer or his/her designee about the incident, including but not limited to: a list of users impacted, a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

iv. Vendor acknowledges that upon initial notification from Vendor, the District has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide such notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform the Data Protection Officer or his/her designee.

v. Vendor will cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

vi. Vendor will pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor, its subcontractors or assignees.

4. Additional Statutory and Regulatory Obligations

Vendor acknowledges additional obligations under Section 2-d and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and these Terms and Conditions. Vendor acknowledges and agrees to the following:

- i. To limit internal access to Protected Data to only those employees or subcontractors that need access to the Protected Data in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.
- ii. To not use Protected Data for any purposes not explicitly authorized in the Master Agreement or these Terms and Conditions.
- iii. To not disclose any Protected Data to any other party, except for authorized employees, subcontractors, or assignees of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:
 - a. the parent or eligible student provided prior written consent;or
 - b. the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- iv. To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.
- v. To use encryption to protect Protected Data in its custody while in motion and at rest, using a technology or methodology specified or permitted by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.
- vi. To adopt technologies, safeguards and practices that align with the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, "NIST Cybersecurity Framework" (Version 1.1).
- vii. To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

D. PARENTS' BILL OF RIGHTS AND SUPPLEMENTAL INFORMATION

1. Parents' Bill of Rights

Vendor acknowledges and agrees that the District's Parents' Bill of Rights as set forth herein and as posted on the District's website is incorporated into these Terms and Conditions.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Orchard Park Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- 2) Parents have the right to inspect and review the complete contents of their child's education record.
- 3) State and federal laws protect the confidentiality of personally identifiable information, 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 New York State is available for public review at the following website <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure..>

John Kiser

Signature

John Kiser, Director of Information Technology
Language Testing International, Inc.

Feb 13, 2023

Date

Sarah Hornung

Sarah Hornung, Director of Technology & CIO
Orchard Park CSD

Date: 02/13/2023

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Orchard Park Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.

2. Supplemental Information

- i. The exclusive purpose for which Protected Data will be used: ~~is ACTFL OPI & WPT for the Seal of Biliteracy® Test Portal~~. Vendor will not use the

Protected Data for any other purposes not explicitly authorized herein or within the Master Agreement.

ii. In the event that Vendor engages subcontractors or other authorized persons or entities (“Subcontractors”) to perform one or more of its obligations under the Master Agreement (including hosting of the Protected Data), Vendor will require Subcontractors to execute legally binding agreements acknowledging and agreeing to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement, these Terms and Conditions, and applicable state and federal law and regulations.

iii. The Master Agreement commences on 02/10/2023 and expires on 06/30/2026. Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will (select all that apply):

Securely delete or otherwise destroy all Protected Data remaining in the possession of Vendor or any of its Subcontractors.

Assist the District in exporting and returning all Protected Data previously received to the District in such formats as may be requested by the District.

Contact the District requesting instruction for the deletion or return of all Protected Data.

In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any Subcontractors will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or Subcontractors will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

iv. Parents or eligible students can challenge the accuracy of any Protected Data in accordance with the District’s procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District’s applicable APPR Plan.

v. Any Protected Data will be stored on systems maintained by Vendor, or Subcontractor(s) under the direct control of Vendor, in a secure data center facility. The measures that Vendor (and, if applicable, Subcontractor(s)) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure

Cybersecurity, “NIST Cybersecurity Framework” (Version 1.1) and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

vi. Vendor (and, if applicable, Subcontractor(s)) will use encryption to protect Protected Data in its custody while in motion and at rest, using a technology or methodology specified or permitted by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

3. Posting

In accordance with Section 2-d, the District will publish the Parents’ Bill of Rights and Supplemental Information from these Terms and Conditions on its website. The District may redact the Parents’ Bill of Rights and Supplemental Information to the extent necessary to safeguard the privacy and/or security of the District’s data and/or technology infrastructure.

IN WITNESS WHEREOF, the Parties have indicated their acceptance of these Terms and Conditions including the Parents' Bill of Rights and Supplemental Information by their signatures below on the dates indicated.

BY THE VENDOR:

John Kiser
Name (Print)

John Kiser

Signature

Director of Information Technology
Title

Feb 13, 2023

Date

BY THE DISTRICT:

Sarah Hornung

Name (Print)

Sarah Hornung

Signature

Director of Technology & CIO

Title

02/13/2023

Date

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	<p>Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.</p>	<p style="color: red;">By maintaining our current data security and privacy protocols and best practices as described below.</p> <p style="color: red;">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.</p> <p style="color: red;">As part of its standard best practices regarding data security,</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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. <p style="color: red;">LTI uses technology, safeguards, and practices that align with the NIST Cybersecurity Framework (Version 1.1).</p> <p style="color: red;">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.</p>
2	<p>Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.</p>	<p style="color: red;">LTI employees are assigned roles on a need-to-know basis.</p> <p style="color: red;">PII data stored in databases are AES 256-bit encrypted.</p> <p style="color: red;">LTI's infrastructure & web applications are beyond well architected solutions and firewalls that deny all network traffic except SSL (TLS 1.2).</p> <p style="color: red;">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:</p> <ul style="list-style-type: none"> • Users' need for access

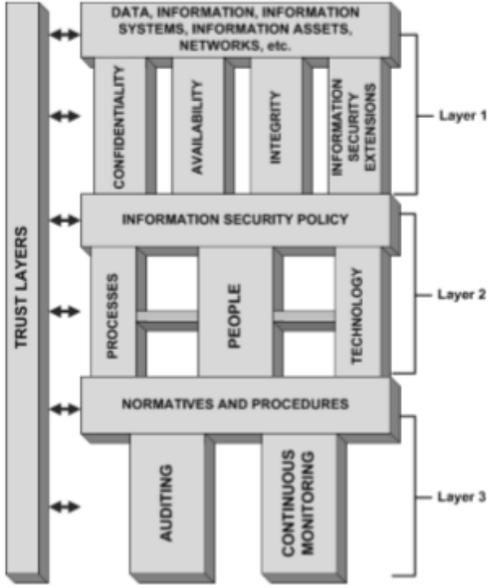
		<ul style="list-style-type: none"> • Potential conflict with segregation of duties • Any regulatory requirements • Level of access required (read, update, delete) • Period for access. <p>User Account review Process: User Account monitoring and management controls provide a gatekeeper function to prevent 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.</p> <p>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.</p>
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.	<p>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.</p> <p>All LTI developers follow secure coding practices, and all development takes into account the most current OWASP guidelines.</p> <p>LTI developers are required to undergo a secure coding training program at least every 12 months.</p> <p>New IT employees must undergo their 1st secure coding training program 6–12 months after their hire date.</p>
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.	<p>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."</p> <p>LTI sub-contractors must sign a similar NDA.</p>
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.	<p>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.</p> <p>LTI will cooperate with the EA and provide as much information as possible, including but not limited to:</p> <ul style="list-style-type: none"> • 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,

		<ul style="list-style-type: none"> 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.	<p>LTI's Process for Destruction of Client Data</p> <ol style="list-style-type: none"> 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.) After confirmation that the EA's testing account has been paid in full, LTI will initiate a data destruction request. The data are destroyed. The data destruction is internally validated. <p>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.</p>
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	<p>LTI is in compliance with the Contractor responsibilities as stated in the Third-Party Contractor Responsibilities section (p. 7) of 5676 Privacy and Security for Student Teacher and Principal Data Updated found at https://www.opschools.org//cms/lib/NY02208923/Centricity/Domain/35/5676%20%20Privacy%20and%20Security%20for%20StudentTeacher%20and%20Principal%20Data%20Updated.pdf. If more information is required, please clarify.</p>
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)	<p>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.</p>	<p>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.</p> <p>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:</p> <ol style="list-style-type: none"> 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
	<p>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.</p>	<p>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.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Users’ need for access • Potential conflict with segregation of duties • Any regulatory requirements • Level of access required (read, update, delete) • Period for access
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational</p>	<p>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.</p>

Function	Category	Contractor Response
	<p>requirements are understood and inform the management of cybersecurity risk.</p>	<p>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.</p> 
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>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.</p>
	<p>Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>The management team evaluates on a periodic basis the threat landscape and our risks and considers how to proceed with due diligence.</p>
	<p>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.</p>	<p>N/A</p>

**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

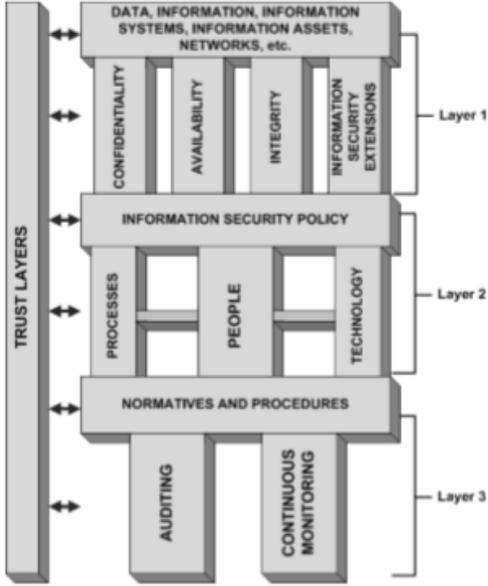
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

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.

	<p>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.</p>	<p>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.</p> <p>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.</p> 
	<p>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.</p>	<p>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.</p>
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>N/A - AWS</p>
	<p>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.</p>	<p>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.</p>
<p>DETECT (DE)</p>	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>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.</p>
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>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.</p>

	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.
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.

Language Testing Intl Master Terms and Conditions Ex. A, C, C.1_for John to sign

Final Audit Report

2023-02-13

Created:	2023-02-13
By:	Allen Bernier (abernier@languagetesting.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAtxHaoM0QdHugQmxjh3YHqxcUdtK8Erlu

"Language Testing Intl Master Terms and Conditions Ex. A, C, C.1_for John to sign" History

-  Document created by Allen Bernier (abernier@languagetesting.com)
2023-02-13 - 2:37:49 PM GMT- IP address: 97.83.163.132
-  Document emailed to John Kiser (jkiser@languagetesting.com) for signature
2023-02-13 - 2:39:12 PM GMT
-  Document e-signed by John Kiser (jkiser@languagetesting.com)
E-signature obtained using URL retrieved through the Adobe Acrobat Sign API
Signature Date: 2023-02-13 - 10:47:40 PM GMT - Time Source: server- IP address: 50.39.123.34
-  Agreement completed.
2023-02-13 - 10:47:40 PM GMT



Sarah Hornung
Director of Technology & CIO
Orchard Park CSD
e-signature date: 02/13/2023