Vendor Questionnaire (Data Privacy Agreement): 285606

Created Date: 3/28/2022 8:19 AM Last Updated: 4/19/2022 8:56 AM

Directions

Below is the Third Party contact that will fill out the Part 121//DPA questionnaire. If this is accurate, click the blue "Publish" button. If not, select the appropriate contact by clicking "Lookup" or create a new contact by clicking "Add New".

Vendor Compliance Contacts

Name (Full)	Email	Phone	Third Party Profile
Art Graham	artg@mlasolutions.com		Mandarin Library Automation
Jon Edwards	jone@mlasolutions.com		
Mario Martinez	mariom@mlasolutions.com		

General Information

Third Party Profile:	Mandarin Library Automation	**Overall Status:**	Approved
Questionnaire ID:	285606	**Progress Status:**	100%
Engagements:	Mandarin Library Automation (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	4/12/2022	**Submit Date:**	4/12/2022
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	4/19/2022
Reviewer Comments:			
Unlock Questions for Updates?:	Assessment questions are set to read-only by default as the assessment should be completed by a vendor through the vendor portal. Do you need to unlock the questionnaire to manually make an update to the submitted questions? This field should be reset to null after the update is made, prior to existing the record.		

Data Privacy Agreement and NYCRR Part 121

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 pre-kindergarten 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.

NYCRR - 121.3 (b)(1):	What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	Specifically and exclusively for library management purposes.
NYCRR - 121.3 (b)(2):	Will the organization use subcontractors? If so, how will the organization 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 State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d, NIST Cybersecurity Framework)?	No. We do not use any subcontractors regarding student teacher or principle data.
NYCRR - 121.3 (b)(3):	What is the duration of the contract including the contract's expected commencement and expiration date? If no contract applies, describe how to terminate the service. Describe what will happen to the student data or teacher or principal data upon expiration. (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be securely destroyed and how all copies of the data that may have been provided to 3rd parties will be securely destroyed)	The duration of the contract is in alignment with NY state DREAM contract. All data can be returned to the school in a MARC records or delimited format. We would then permanently remove all data, transactions our servers. We do not provide an patron data to any 3rd party for any reason.

NYCRR - 121.3 (b)(4):	How can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected?	Typically the parent, student, teacher or principal data accuracy would be determined by the school administration or librarian/teacher or designated school official.
NYCRR - 121.3 (b)(5):	Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.	Data will be stored on servers located on our premises. We uses AES 256-bit encryption on stored password data. In addition, usernames and passwords are encrypted with AES 256-bit encryption before being sent over the wire. This is in addition to the encryption provided by SSL below. We currently use: AES 256 over TLS 1.2 with 3072-bit key size. The 2048 above refers to the key size. Some SSL certificates, for example, Amazon.com, are using only AES 128 with 2048-bit key size. Support staff have no ability to read a stored password. Passwords can be reset by an admin with access. Other Patron data is viewable by persons with admin-level access.
NYCRR - 121.3 (b)(6):	Please describe how and where encryption is leveraged to protect sensitive data at rest and while in motion. Please confirm that all encryption algorithms are FIPS 140-2 compliant.	Usernames and passwords are stored using AES 256-bit encryption. Data is transmitted over the wire using TLS 1.2 encryption. Usernames and passwords are encrypted using AES 256 before being transmitted over SSL.
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	DataProtectionPolicy.pdf
NYCRR - 121.6 (a)(1):	Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy.	The organization will implement all requirements set forth by local, state, and Federal governments.
NYCRR - 121.6 (a)(2):	Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.	All personally identifible information is stored with encryption and/or transmitted over the wire in encrypted format. No third parties are involved in handling personally identifiable information. Only a handful of trained employees have access to such information and it is handled under the same security as valuable intellectual property.
NYCRR - 121.6 (a)(4):	Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access.	Technical support representatives will receive in person and remote training from technical support management and QA.
NYCRR - 121.6 (a)(5):	Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.	We do not use subcontractors that involve patron PII data.
NYCRR - 121.6 (a)(6):	Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency.	If there is a confirmed security breach, Mandarin Library Automation, will contact the affected NY/school officials within 24 hours. We will call and/or email.
NYCRR - 121.6 (a)(7):	Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. Vendor will be required to complete a Data Destruction Affidavit upon termination of the engagement.	We can return PII data to the school admin or designated contact however and whenever requested. We can then purge PII data.
NYCRR - 121.9 (a)(1):	Is your organization compliant with the NIST Cyber Security Framework?	Yes
NYCRR - 121.9 (a)(2):	Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law section 2-d; and this Part.	The organization will implement all security and privacy policy requirements of the educational agency.

NYCRR - 121.9 (a)(3):	Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need authorized access to provide services.	Access. login and password information is only used by QA and trained technical support representatives.
NYCRR - 121.9 (a)(4):	Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract. (e.g. Role Based Access, Continuous System Log Monitoring/Auditing)	Access to PII is exclusively accessed by trained technical support representatives, management and QA. Access to such data is only available via login and password.
NYCRR - 121.9 (a)(5):	Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or (ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	We would not disclose any PII to any sub contractor as we do not use sub contractor regarding PII. We would only provide PII to state and /or federal requirements based on a court order.
NYCRR - 121.9 (a)(6):	Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.	The organization imposes rigorous safeguards on data and employee access.
NYCRR - 121.9 (a)(7):	Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.	We uses AES 256-bit encryption on stored password data. In addition, usernames and passwords are encrypted with AES 256-bit encryption before being sent over the wire. This is in addition to the encryption provided by SSL below. We currently use: AES 256 over TLS 1.2 with 3072-bit key size. The 2048 above refers to the key size. Some SSL certificates, for example, Amazon.com, are using only AES 128 with 2048-bit key size. Support staff have no ability to read a stored password. Passwords can be reset by an admin with access. Other Patron data is viewable by persons with admin-level access.
NYCRR - 121.9 (a)(8):	Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	Affirm
NYCRR - 121.9 (a)(b):	Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	We do not use sub contractors in any phase of our hosting environment.
NYCRR - 121.10 (a):	Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	If a confirmed breach occurs Mandarin Library Automation will notify designated school administration, librarian/teacher and BOCES director. We would call and/or email based on the fastest method to notify.
NYCRR - 121.10 (f):	Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	Affirm
NYCRR - 121.10 (f.2):	Please identify the name of your insurance carrier and the amount of your policy coverage.	AutoOwner Insurance - General Liability - $2,000,000.00
NYCRR - 121.10 (c):	Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	Affirm

Acceptable Use Policy Agreement:	Do you agree with the Capital Region BOCES Acceptable Use Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BU4QYA6B81BF)	I Agree
Privacy Policy Agreement:	Do you agree with the Capital Region BOCES Privacy Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BWZSQ273BA12)	I Agree
Parent Bill of Rights:	Please upload a signed copy of the Capital Region BOCES Parent Bill of Rights. A copy of the Bill of Rights can be found here: https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf	Parent Bill of Rights.pdf
DPA Affirmation:	By submitting responses to this Data Privacy Agreement the Contractor agrees to be bound by the terms of this data privacy agreement.	I Agree

Attachments

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details

Contact Name:	The Risk Mitigation & Compliance Office	**Publish Date:**	
Required Portal Fields Populated:	Yes	**Contact Email Address:**	crbcontractsoffice@neric.org
About NYCRR Part 121:	In order for a vendor to engage with a New York State Educational Agency, the vendor must provide information required by the New York State Commissioner's Regulations Part 121 (NYCRR Part 121) and the National Institute of Standards and Technology Cyber Security Framework. If deemed appropriate, the responses you provide will be used as part of the data privacy agreement between the vendor and the Albany-Schoharie-Schenectady-Saratoga BOCES. This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and Mandarin Library Automation ("CONTRACTOR"), collectively, the "Parties". 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.	**Requesting Company:**	Capital Region BOCES
Created By:		**Third Party Name:**	Mandarin Library Automation
		Name:	Mandarin Library Automation-285606