Vendor Questionnaire (Data Privacy Agreement): 278468

Created Date: 11/1/2021 2:10 PM Last Updated: 11/15/2021 4:22 PM

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
Judith Koss	Judie@SAFARIMontage.com		Library Video Company d/b/a SAFARI Montage
Erin Gold	egold@safarimontage.com		

General Information

Third Party Profile:	Library Video Company d/b/a SAFARI Montage	**Overall Status:**	Approved
Questionnaire ID:	278468	**Progress Status:**	100%
Engagements:	Library Video Company d/b/a SAFARI Montage (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	11/16/2021	**Submit Date:**	11/15/2021
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	11/15/2021
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?	The exclusive purpose for which SAFARI Montage is receiving and will use Protected Data (i.e., Student Data and Teacher or Principal Data) from BOCES is to provide BOCES with the functionality of the products and services provided by SAFARI Montage.

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)?	In the event that SAFARI Montage engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of SAFARI Montage under the AGREEMENT and applicable state and federal law. SAFARI Montage will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Consistent with our written information security program, which SAFARI Montage will maintain during the term of the MLSA, SAFARI Montage will vet each of its authorized subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) with respect to their data security practices, periodically review the subcontractors or other authorized person or entities and their compliance with the program, and request relevant data security requirements in agreements, where feasible.
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 Effective Date of this Agreement is July 1, 2021. The initial term of this Agreement shall commence on the effective date and continue until June 30, 2022. At the end of the initial one year contract term upon mutual agreement of the Parties, the agreement may be renewed for two (2) additional years, in two (2) consecutive one-year intervals. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, SAFARI Montage will securely delete or otherwise destroy any and all Protected Data remaining in the possession of SAFARI Montage or its assignees or subcontractors. If requested by a Participating Educational Agency, SAFARI Montage will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion. Any destruction of data will be directed by BOCES or the Participating Educational Agency to which the data belongs. At BOCES request, SAFARI Montage will cooperate with BOCES as necessary in order to transition Protected Data to any successor SAFARI Montage prior to deletion. SAFARI Montage agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, SAFARI Montage and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full. Subcontractors will provide a certification of destruction where feasible. Vendor may retain de-identified or anonymized data.

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?	Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to SAFARI Montage, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to SAFARI Montage by following the appeal process in their employing school district's applicable APPR Plan.
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.	Any Protected Data SAFARI Montage receives will be stored on systems maintained by SAFARI Montage, or by a subcontractor under the direct control of SAFARI Montage, in a secure data center facility located within the United States. The measures that SAFARI Montage will take to protect Protected Data include adoption of reasonable technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
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.	SAFARI Montage encrypts all student data in transit using SSL and at rest using 256-bit AES, one of the strongest block ciphers available. Azure and AWS cloud storage encryption is enabled for all storage accounts. Server-side encryption (SSE) automatically encrypts data stored on Azure- or AWS-managed disks (OS and data disks) at rest by default when persisting it to the cloud. Data in Azure- or AWS-managed disks are encrypted transparently using 256-bit AES and is FIPS 140-2 compliant. SAFARI Montage also appropriately secures all physical media containing student data during backup, transport, storage, and destruction using 256-bit AES encryption or greater. SAFARI Montage (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	LibraryVideoCoDREAMAssessVendorQuestNYCRR121.6(a).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.	In order to implement all state, federal, and local data security and privacy requirements, including those contained within the DPA, consistent with BOCES data security and privacy policy, SAFARI Montage will maintain a comprehensive information security program as described in Section 7 of its Products and Services Privacy Policy ("Privacy Policy"). In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the SAFARI Montage AGREEMENT, SAFARI Montage will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the SAFARI Montage AGREEMENT: maintain a comprehensive information security program as described in Section 7 of its Privacy Policy.
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.	SAFARI Montage maintains strict access controls to all systems involved in granting access to student data and personally identifiable information. Technical support systems are restricted to personnel requiring access to perform their job functions. Two-factor authentication is enabled for remote VPN access, Microsoft 365 email, productivity applications, storage, and cloud services. We encrypt all student data in transit using SSL and at rest using 256-bit AES, one of the strongest block ciphers available. Azure and AWS cloud storage encryption is enabled for all storage accounts. Server-side encryption (SSE) automatically encrypts data stored on Azure- or AWS-managed disks (OS and data disks) at rest by default when persisting it to the cloud. Data in Azure- or AWS-managed disks are encrypted transparently using 256-bit AES and is FIPS 140-2 compliant. Passwords are encrypted in data storage locations and password entry fields are obfuscated in entry interfaces controlled by the discloser. User authentication at login occurs using at least 128-bit AES encryption. Data entered during authentication is secured in transit using https/TLS 1.0+, secure FTP services, or SSH.
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.	We believe that information security awareness and adherence to our policies and procedures is the responsibility of every employee. We ensure that all employees are adequately trained regarding data privacy (such as FERPA, COPPA, and state laws) and security awareness upon hire and on an ongoing basis. Our training includes conducting unannounced simulated phishing exercises to continually improve our security competence. Individual and organizational training compliance is documented and analyzed in order to identify and mitigate areas of weakness.

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.	In the event that SAFARI Montage engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of SAFARI Montage under the AGREEMENT and applicable state and federal law. SAFARI Montage will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Consistent with our written information security program, which SAFARI Montage will maintain during the term of the MLSA, SAFARI Motnage will vet each of its authorized subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) with respect to their data security practices, periodically review the subcontractors or other authorized person or entities and their compliance with theprogram, and request relevant data security requirements in agreements, where feasible.

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.	SAFARI Montage shall promptly notify BOCES of any confirmed 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 SAFARI Montage has discovered or been informed of the breach or unauthorized release. SAFARI Montage will provide such notification to BOCES by contacting the BOCES Data Privacy Officer, at michele.jones@neric.org. SAFARI Montage will cooperate with BOCES and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date SAFARI Montage discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what SAFARI Montage 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 SAFARI Montage representatives who can assist affected individuals that may have additional questions. SAFARI Montage acknowledges that upon initial notification from SAFARI Montage, BOCES, as the educational agency with which SAFARI Montage contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department (“CPO”). SAFARI Montage shall not provide this notification to the CPO directly. In the event the CPO contacts SAFARI Montage directly or requests more information from SAFARI Montage regarding the incident after having been initially informed of the incident by BOCES, SAFARI Montage will promptly inform the Data Protection Officer or designees. SAFARI Montage will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

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.	Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, SAFARI Montage will securely delete or otherwise destroy any and all Protected Data remaining in the possession of SAFARI Montage or its assignees or subcontractors. If requested by a Participating Educational Agency, SAFARI Montage will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion. Any destruction of data will be directed by BOCES or the Participating Educational Agency to which the data belongs. At BOCES request, SAFARI Montage will cooperate with BOCES as necessary in order to transition Protected Data to any successor SAFARI Montage prior to deletion. SAFARI Montage agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, SAFARI Montage and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full. Subcontractors will provide a certification of destruction where feasible. Vendor may retain de-identified or anonymized 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.	SAFARI Montage will comply with all terms, conditions, and obligations as set forth in the Data Privacy Agreement incorporated in the the Master License and Service Agreement.
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.	SAFARI Montage maintains strict access controls to all systems involved in granting access to student data and personally identifiable information. Technical support systems are restricted to personnel requiring access to perform their job functions. Two-factor authentication is enabled for remote VPN access, Microsoft 365 email, productivity applications, storage, and cloud services. We structure our employee on- and off-boarding processes to ensure that employee access to customer and privileged systems is granted solely on least access security needs, adjusted appropriately upon any change of responsibility, and terminated immediately upon separation from the company.

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)	SAFARI Montage maintains strict access controls to all systems involved in granting access to student data. Technical support systems are restricted to personnel requiring access to perform their job functions. Two-factor authentication is enabled for remote VPN access, Microsoft 365 email, productivity applications, storage, and cloud services. We encrypt all student data in transit using SSL and at rest using 256-bit AES, one of the strongest block ciphers available. Azure and AWS cloud storage encryption is enabled for all storage accounts. Server-side encryption (SSE) automatically encrypts data stored on Azure- or AWS-managed disks (OS and data disks) at rest by default when persisting it to the cloud. Data in Azure- or AWS-managed disks are encrypted transparently using 256-bit AES and is FIPS 140-2 compliant. SAFARI Montage maintains logs and records of all employee support access to customer systems through privileged technical support access methods. SAFARI Montage applications log and record notable events, including successful and failed logins, direct logins, remote logins, and system access from third-party LMS, systems, or from permanent links. Audit logs include time, date, user account, details of action, source IP address, and other information relevant to profiling system activities, all of which enables the monitoring, analysis, investigation, and reporting of unauthorized system activity. Customers maintain control over audits with respect to their internal users and manage any access granted to SAFARI Montage employees for support and maintenance reasons via customer-provided user accounts, including access, authentication, and audit controls.
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.	Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to SAFARI Montage, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to SAFARI Montage by following the appeal process in their employing school district’s applicable APPR Plan.

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.	SAFARI Montage maintains strict access controls to all systems involved in granting access to student data. Technical support systems are restricted to personnel requiring access to perform their job functions. Two-factor authentication is enabled for remote VPN access, Microsoft 365 email, productivity applications, storage, and cloud services. We encrypt all student data in transit using SSL and at rest using 256-bit AES, one of the strongest block ciphers available. Azure and AWS cloud storage encryption is enabled for all storage accounts. Server-side encryption (SSE) automatically encrypts data stored on Azure- or AWS-managed disks (OS and data disks) at rest by default when persisting it to the cloud. Data in Azure- or AWS-managed disks are encrypted transparently using 256-bit AES and is FIPS 140-2 compliant. SAFARI Montage maintains logs and records of all employee support access to customer systems through privileged technical support access methods. SAFARI Montage applications log and record notable events, including successful and failed logins, direct logins, remote logins, and system access from third-party LMS, systems, or from permanent links. Audit logs include time, date, user account, details of action, source IP address, and other information relevant to profiling system activities, all of which enables the monitoring, analysis, investigation, and reporting of unauthorized system activity. Customers maintain control over audits with respect to their internal users and manage any access granted to SAFARI Montage employees for support and maintenance reasons via customer-provided user accounts, including access, authentication, and audit controls.
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.	SAFARI Montage encrypts all Protected Data in transit using SSL and at rest using 256-bit AES, one of the strongest block ciphers available. Azure and AWS cloud storage encryption is enabled for all storage accounts. Server-side encryption (SSE) automatically encrypts data stored on Azure- or AWS-managed disks (OS and data disks) at rest by default when persisting it to the cloud. Data in Azure- or AWS-managed disks are encrypted transparently using 256-bit AES and is FIPS 140-2 compliant. SAFARI Montage also appropriately secures all physical media containing Protected Data during backup, transport, storage, and destruction using 256-bit AES encryption or greater. SAFARI Montage physically secures all systems involved in supporting and accessing customer systems with privileged access not provided directly by customers. Internal systems are physically secured via least privilege access controls ranging from door (depending on the facility) access key codes to biometric palm and retinal scanning. For SAFARI Montage cloud installations operating on Azure and AWS platforms, data centers managed by those entities comply with a broad set of international and industry-specific compliance standards and validations, such as NIST SP 800-171, ISO 27001, SOC 1, and SOC 2.

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.	In the event that SAFARI Montage engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of SAFARI Montage under the AGREEMENT and applicable state and federal law. SAFARI Montage will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Consistent with our written information security program, which SAFARI Montage will maintain during the term of the MLSA, SAFARI Motnage will vet each of its authorized subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) with respect to their data security practices, periodically review the subcontractors or other authorized person or entities and their compliance with the program, and request relevant data security requirements in agreements, where feasible.
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.	SAFARI Montage has a formal cyber incident response plan that provides the processes, procedures, and timelines or security breach notifications. Per SAFARI Montage's cyber incident response plan, if notification is required all customers, vondors, and business partners are to be notified with 24 hours of discovery.
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.	A certificate of liability insurance is attached.
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	CRBOCES Parents Bill of Rights-Vendors.FE.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
LVC dba SAFARI Montage - Insurance Certificate.pdf	99365	.pdf	11/15/2021 2:46 PM	0

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 Library Video Company d/b/a SAFARI Montage ("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:**	Library Video Company d/b/a SAFARI Montage
		Name:	Library Video Company d/b/a SAFARI Montage-278468