Vendor Questionnaire (Data Privacy Agreement): 280708
Created Date: 1/3/2022 1:11 PM Last Updated: 1/14/2022 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
Dianah Tsilifonis	dtsilifonis@ebsco.com		EBSCO Information Services
RFP Team	rfpalerts@ebsco.com		EBSCO Information Services
Duane Elbrecht	delbrecht@ebsco.com		EBSCO Information Services
Tyler Smith	tsmith1@ebsco.com		EBSCO Information Services

General Information

Third Party Profile:	EBSCO Information Services	**Overall Status:**	Approved
Questionnaire ID:	280708	**Progress Status:**	100%
Engagements:	EBSCO Information Services (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	1/18/2022	**Submit Date:**	1/13/2022
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	1/14/2022
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?	EBSCO uses the Personal Information we collect for the limited purposes of processing your transactions, establishing and/or verifying a person's or account holder's identity, customer service, improving and customizing our Services and their content, authorization, content processing, content classification, and providing you with information concerning our Services.
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 situations where we share Personal Information with Service Providers, we ensure access is granted to the Service Providers only upon the condition that the Personal Information is kept confidential and is used only for carrying out the services these Service Providers are performing for EBSCO. As part of making that determination whether we will share Personal Information with Service Providers, we will obtain assurances that they will appropriately protect and maintain the confidentiality of Personal Information consistent with our Privacy Policy and as required by applicable law. In addition, we have a comprehensive vendor risk assessment program, and require vendors to sign data protection agreements where applicable.
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 expected to be one base year, with the option to renew for two additional years, at the DREAM consortium's discretion. Exact dates are to be determined. EBSCO will only retain information for as long as your account is active, or as needed to provide you Services, comply with our legal obligations, resolve disputes, and enforce our agreements. Upon contract termination and written request, data will be deleted or anonymized. If this is not possible (e.g., because the information has been stored in backup archives), then EBSCO will securely store, protect as production, and isolate the information from any further processing, until deletion is possible. However, de-identified data may be retained for business intelligence purposes. All information can also be returned to the customer upon written request, or in accordance with the license agreement. EBSCO will provide the data in a mutually agreed upon format, or the original format it was provided in. Regarding third parties, EBSCO obtains assurance that any Service Providers will appropriately protect and maintain the confidentiality of Personal Information consistent with our Privacy Policy and as required by applicable law.
NYCRR - 121.3(b)	How can a parent, student, eligible student, teacher or principal	If a user would like to manage, change, limit or

(4):	challenge the accuracy of the student data or teacher or principal data that is collected?	delete their Personal Information, they may do so through their account settings within EBSCO services, or by submitting a request using any of the methods provided in EBSCO's Privacy Policy (https://www.ebsco.com/company/privacy-policy#prod_what-are-my-rights).
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 within Amazon's AWS East Region 1, as well as within EBSCO's data centers located in the greater Boston, MA area. EBSCO maintains extensive information security policies to protect data which focuses on web application security and includes firewall and router security, data classification and control, vulnerability identification, authentication, etc. EBSCO also keeps audit trails to maintain records of system activity both by system and application processes and by user activity, which, in conjunction with appropriate tools and procedures, acts as a technical control facilitating the detection of security violations, performance issues, etc.
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.	All sensitive data is securely encrypted in the database with restricted access, using AES-256. Data is also encrypted in transit with SSL/TLS1.2 2048-bit encryption (which is FIPS 140-2 compliant). Encryption for data in motion (HTTPS) is enabled by default; it can enabled/disabled by the customer through EBSCOadmin (the online administration module).
NYCRR - 121.6(a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Information Security Whitepaper_EBSCO Rev. April 2020 (5).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.	EBSCO strives to comply with all local, state and federal security and privacy requirements and continually monitors changes to laws and regulations. EBSCO will make changes to security and privacy policies when necessary to ensure our services and practices align with evolving requirements.
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.	EBSCO's information security and infrastructure teams focus on the confidentiality, integrity and availability of our information and systems. This approach uses a multitude of monitoring tools, processes and procedures to control access (user authentication and logical access controls); protect and prevent intrusions (antivirus software, firewalls, etc.); and identify, track, monitor and report on pertinent security events. The information security incident management approach addresses any significant event, which includes communicating to all relevant individuals/groups within EBSCO for identification, categorization, analysis, remediation and monitoring. Both EBSCOhost and LearningExpress are ISO 27001 certified. EBSCO's certificate can be found at https://www.schellman.com/certificate-directory (search for 'EBSCO' to locate).
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.	EBSCO's security policies are designed to comply with various federal and state regulations. Employees are trained on best practices and provided a number of security trainings related to data protection, phishing risks, acceptable use, etc. Employees receive additional and follow-up training based on role, and refresher trainings are provided via EBSCO's online learning management platform.
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 situations where we share Personal Information with Service Providers, EBSCO ensures access is only granted upon the condition that the Personal Information is kept confidential and is only used for carrying out the services performed for EBSCO. As part of making that determination whether we will

		share Personal Information with Service Providers, EBSCO will obtain assurances that they will appropriately protect and maintain the confidentiality of Personal Information consistent with our Privacy Policy and as required by applicable law.
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.	EBSCO employs internal monitoring across environments with multiple tools to identify, track, monitor and report on pertinent risks and vulnerabilities (e.g., security events). Monitoring tools are set up to provide alarms and notices to EBSCO staff. EBSCO has an incident management approach that ensures any security events are handled accordingly. This involves ensuring incident response procedures are followed in order to contain or eradicate any threats or issues, taking due diligence in investigating and reporting the incident, taking appropriate steps to recover from the incident, and, if necessary, taking appropriate steps to escalate issues to senior management, law enforcement or other key stakeholders. Events that directly impact customers are highest priority. EBSCO will notify customers within 72 hours of discovery if a security incident has impacted its data. Post-event assessments are conducted to determine the root cause for events, regardless of threat, to understand if the causes are one-time, or trends, to adjust response or prevent recurrence. Incident management procedures are also exercised based on threat scenarios (e.g., insider threats, phishing, social engineering, software vulnerabilities) as needed to ensure that processes are efficient, and stakeholders understand protocol.
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.	If a customer provides data to EBSCO for use in the service, the customer may request that the data be returned at the end of the contract. EBSCO will provide the data in a mutually agreed upon format, or the original format it was provided in. Please note that EBSCO will only receive a copy of this data; the original copy will be maintained by the customer. Upon contract termination, customers may request that all data associated with the service be removed from EBSCO's services. EBSCO will securely delete the data and provide the customer with an attestation that the data has been removed.
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.	EBSCO's information security and infrastructure teams focus on the confidentiality, integrity and availability of our information and systems. This approach uses a multitude of monitoring tools, processes and procedures to control access (user authentication and logical access controls); protect and prevent intrusions (antivirus software, firewalls, etc.); and identify, track, monitor and report on pertinent security events. EBSCO strives to comply with all local, state and federal security and privacy requirements and continually monitors changes to laws and regulations. EBSCO will make changes to our security and privacy policies when necessary to ensure services and practices align with evolving requirements.
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.	EBSCO has taken appropriate technical and organizational measures to ensure that Personal Information we have collected or will collect in the future is secure. For example, we have limited the number of people who have access to Personal Information, by electronic security systems and authentication methods that guard against unauthorized access. EBSCO also maintains

		detailed logical access control security, with employees provisioned based on job role under the principle of least privilege. Employee access to the system is requested by management and approved by EBSCO's Information Security team prior to confirmation. Group access is used to grant employees access based upon their assigned function and job responsibility. If an employee changes role, access rights are reviewed and changed accordingly. Processes and technology are in place to ensure that appropriate changes are made within 24 hours of personnel changes, including full termination in the event of an employee leaving the company. EBSCO limits the number of administrative accounts to the minimum necessary to reduce risk, and reviews are conducted on a periodic basis.
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)	EBSCO has taken appropriate security measures to protect against the loss, misuse or alteration of information that we have collected from you in connection with our Services. As part of this, we implement an extensive information security policy which focuses on web application security (to identify potential or realized weaknesses as a result of inadvertent misconfiguration, authentication, application logic, error handling, sensitive information leakage, etc.). This policy includes firewall and router security, data classification and control, vulnerability identification, authentication, encryption, etc. EBSCO also keeps audit trails to maintain records of system activity both by system and application processes and by user activity, which, in conjunction with appropriate tools and procedures, acts as a technical control facilitating the detection of security violations, performance issues, etc. Moreover, EBSCO maintains detailed logical access control security, with employees provisioned based on job role under the principle of least privilege. Information security training is provided based on these roles and responsibilities, detailing how to handle and secure information assets.
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.	EBSCO may use the Personal Information and non-Personal Information we collect by sharing it with third-party agents, vendors, contractors, partners or content providers of EBSCO (collectively, "Service Providers"). We would do this for purposes of managing purchases of our products and services, providing subsequent access, servicing our systems, and obtaining support services for our businesses. We are not in the business of selling Personal Information to third-parties or Service Providers and will share it with Service Providers only as described in our Privacy Policy. In situations where we share Personal Information with Service Providers, we ensure access is granted to the Service Providers only upon the condition that the Personal Information is kept confidential and is only used for carrying out the services performed for EBSCO. EBSCO also obtains assurance that any Service Providers will appropriately protect and maintain the confidentiality of Personal Information consistent with our Privacy Policy and as required by applicable law. EBSCO does reserve the right to disclose personally identifiable information if required to do so by law, or in the good faith belief that disclosure of the information is reasonably necessary to comply with legal process, to respond to claims, or to protect or advance the rights, property, safety or well-being of the company, our employees, customers or the public. EBSCO will

		inform the institution about any government requests for data or information we receive, unless we are prevented from doing so by law enforcement. Note that several EBSCO K-12 products (e.g., the Explora interface) also comply with COPPA provisions other applicable laws. If a user under 16 years of age wants to use our personalization features, we ask the user to register with their first name (not considered personal information by the US Federal Trade Commission) and a unique identifier only. To the extent we collect any information of minors under 16 years of age that is considered personal information under any applicable law, we do not and will not sell such information without affirmative authorization and have not sold such information during the preceding 12 months or at any other time.
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.	As noted, EBSCO's information security and infrastructure teams focus on the confidentiality, integrity and availability of our information and systems. This approach uses a multitude of monitoring tools, processes and procedures to control access (user authentication and logical access controls); protect and prevent intrusions (antivirus software, firewalls, etc.); and identify, track, monitor and report on pertinent security events. EBSCO data centers also employ a variety of physical security measures, which can include electronic card access control systems; intrusion detectors and alarms; computer inventory control; interior and exterior cameras; and 24/7 security guard access. Additional detail can be found in the attached Information Security Whitepaper. For details regarding physical security measures at AWS facilities, please see https://aws.amazon.com/compliance/data-center/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.	All sensitive data is securely encrypted in the database with restricted access, using AES-256. Data is also encrypted in transit with SSL/TLS1.2 2048-bit encryption (which is FIPS 140-2 compliant), and encryption for data in motion (HTTPS) is enabled by default.
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.	EBSCO uses sub-processors that have been carefully vetted, are periodically assessed and have clearly defined duties and obligations. They have undergone training in the use, care, protection and handling of personal data, and EBSCO uses appropriate contract clauses to ensure they uphold the same obligations to security and privacy that we do.
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.	EBSCO will notify customers via phone and/or email within 72 hours of discovery if its data has been impacted by a security incident.
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.	EBSCO's insurance carrier is Valent Group, LLC. The cyber coverage amount is 5 million dollars.
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	CRB-Parents-Bill-Of-Rights_Vendors.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
SubProcessor List 12-21 (2).pdf	555607	.pdf	1/13/2022 3:17 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 EBSCO Information Services ("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:**	EBSCO Information Services
		Name:	EBSCO Information Services-280708
		Legacy Submit Date:	