

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE
INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	VOCATIONAL EDUCATION AND EXTENSION BOARD OF NASSAU COUNTY
Description of the purpose(s) for which Contractor will receive/access PII	Reporting to the NYS DOH per regulations and course requirements.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date <u>September 1, 2026</u> Contract End Date <u>June 30, 2027</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☒ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: retain only necessary PII to comply with NYS DOH EMS Bureau regulations for a period of seven (7) years following the termination of this agreement.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☐ Using a cloud or infrastructure owned and hosted by a third party.

	☐ Using Contractor owned and hosted solution ☒ Other: Securely stored physical storage device. Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Access to and use of data will be limited to the information necessary to perform the contracted services and only for authorized educational purposes. Access will be restricted to authorized personnel with a legitimate business need. User access will be reviewed periodically and promptly removed when no longer required.
Encryption	Protected data will be encrypted in transit using industry-standard protocols

CONTRACTOR	
[Signature]	<i>John Rottkamp</i>
[Printed Name]	John Rottkamp
[Title]	Executive Director
Date:	8/25/26

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	The Contractor will implement and maintain a comprehensive data privacy and security program throughout the life of the Contract designed to protect PII against unauthorized access, use, disclosure, alteration, loss, or destruction. Throughout the Contract term, the Contractor will: 1. Limit collection, access, use, disclosure, and retention of PII to what is necessary to perform the services authorized by the Contract. 2. Restrict access to PII based upon job responsibilities. 3. Require personnel with access to PII to comply with applicable confidentiality, privacy, and security requirements. 4. Monitor and periodically review access to PII and remove or modify access when it is no longer required. 5. Provide appropriate privacy and security training to personnel with access to PII.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Access to PII is limited to authorized personnel who have a legitimate business need to access the information in order to perform their assigned responsibilities. Physical access to facilities, equipment, and systems containing PII is restricted to

		authorized individuals. PII is encrypted in transit. Secure deletion practices are utilized.
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.	The Contractor provides privacy and information security training to personnel who have access to PII as part of their responsibilities under the Contract. Training is provided before personnel receive access to PII, as appropriate, and periodically thereafter.
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.	Personnel are informed that PII may only be accessed and used for authorized business purposes and may not be disclosed to unauthorized individuals.
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.	The Contractor maintains an incident response process designed to identify, assess, investigate and document actual or suspected security incidents involving PII. Upon identifying a suspected incident involving PII, the Contractor will take reasonable steps to: 1. Identify and assess the nature and scope of the incident; 2. Determine whether PII may have been accessed, acquired, disclosed, altered, lost, or otherwise compromised; 3. Contain and mitigate the incident; 4. Preserve relevant information necessary for investigation; 5. Investigate the cause and scope of the incident; 6. Remediate identified vulnerabilities;

		7. Cooperate with the EA in investigating and addressing the incident; and 8. Document the incident and remediation activities. The Contractor will notify the EA of a breach or unauthorized disclosure involving PII within the time period required by the Contract and applicable law. The Contractor will cooperate with the EA concerning investigation, mitigation, remediation, and legally required notifications.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data will be transferred using appropriate security measures designed to protect PII against unauthorized access or disclosure during the transition. Upon expiration or termination of the Contract, Contractor shall: retain only necessary PII to comply with NYS DOH EMS Bureau regulations for a period of seven (7) years following the termination of this agreement.
7	Describe your secure destruction practices and how certification will be provided to the EA.	The Contractor maintains procedures for secure destruction of PII when it is no longer required for authorized contractual or reporting purposes and when destruction is permitted or required under the Contract and applicable law. The method of destruction will be appropriate to the medium and nature of the information and may include secure electronic deletion, cryptographic erasure where applicable, or physical destruction of storage media when appropriate.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	The Contractor will comply with the EA's applicable Data Security and Privacy Policy and other applicable

		policies incorporated into or referenced by the Contract.
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.

NIST CSF TABLE

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

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	PII is collected strictly for reporting to the NYS DOH per regulations and course requirements. Data is stored on a securely stored physical storage device, and the collection and retention of PII are limited solely to what is necessary for the Contract. Physical access to facilities, equipment, and systems containing PII is restricted to authorized individuals
	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.	PII is accessed and used solely for authorized educational purposes and NYS DOH reporting and course requirements. Access is limited to the information necessary to perform the contracted services.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	The Contractor's program is governed by NYS Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. The Contractor will comply with the Educational Agency's (EA) applicable Data Security and Privacy Policy and other referenced policies.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	The Contractor maintains a data privacy and security program and an incident response process designed to identify, assess, investigate, and document security incidents. User access is reviewed periodically to identify unauthorized access risks.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	PII protections are integrated throughout the contract life cycle to prevent unauthorized access, alteration, or loss.

Function	Category	Contractor Response
PROTECT (PR)	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.	The Contractor will not utilize subcontractors for this contract.
	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.	Access to PII is restricted based on job responsibilities and legitimate business need. Physical access to facility systems is restricted. User access is reviewed periodically and promptly removed when no longer required.
	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.	Privacy and information security training is provided to all personnel with access to PII before they receive access and periodically thereafter. Personnel are informed that PII must only be used for authorized business purposes.
	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.	Data is encrypted in transit using industry-standard protocols. At rest, it is held on a securely stored physical storage device. Upon contract termination, data is retained for 7 years to comply with NYS DOH EMS Bureau regulations and is otherwise destroyed using secure deletion, cryptographic erasure, or physical destruction.
	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.	The Contractor maintains a secure data destruction process, and facilitates corrections to challenged PII within 21 days of receiving a written request from the EA.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance-related access to facility systems and equipment containing PII is mitigated by restricting physical access to authorized individuals only.
	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.	Technical solutions include industry-standard encryption protocols in transit, secure electronic deletion, and cryptographic erasure practices.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Access is continuously monitored.

Function	Category	Contractor Response
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	The Contractor monitors and periodically reviews access to PII. Suspected security incidents are identified and assessed.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Incident response procedures are maintained to identify and assess the nature and scope of suspected incidents, including verifying if PII has been compromised.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	The Contractor maintains an incident response process to manage actual or suspected security incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	The Contractor will notify the EA of a breach or unauthorized disclosure of PII within required timeframes and cooperate on investigations and legally required notifications.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Steps are taken to identify and assess the nature and scope of the incident and investigating the cause of any breaches.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	The Contractor will contain and mitigate the incident, remediate identified vulnerabilities, and cooperate fully with the EA.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Vulnerabilities are remediated, and all incidents and remediation activities are documented to improve future response procedures.
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.	Hard drive recovery protocols are used in the event of a failure of the physical drives.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Lessons from incident documentation are utilized to strengthen recovery protocols.
	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 vendors).	Restoration and remediation activities are coordinated with the EA to ensure alignment with educational agency expectations.