PROVIDER'S DATA PRIVACY AND SECURITY PLAN

Provider 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 School District's website, Provider should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

Name of Provider: _____
Address: _____
Email/Phone: _____

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	What will you do to keep the data you use secure?
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	How do you protect the data that you use? Ex: Secured Electronically, in a locked file cabinet in a locked room, etc.
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.	Describe the training you and/or employees or subcontractors receive in order to keep data secure.
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.	If you have employees or subcontractors, how do you make sure they are keeping the data secure? If you do not have employees or subcontractors, please write n/a.
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 School District.	What do you do if there is a data breach and how do you identify a breach/ unauthorized disclosure? How do you report a breach/unauthorized disclosure to the School District.
6	Describe how data will be transitioned to the School District when no longer needed by you to meet your contractual obligations, if applicable.	Ex: Emailed to the School District, hand delivered, etc.

7	Describe your secure destruction practices and how certification will be provided to the School District.	How do you destroy the data you use and how will you show proof that the data was destroyed?
8	Outline how your data security and privacy program/practices align with the School District's applicable policies.	Describe how your ways of securing data align with the School District's Policies about data security.
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

Providers 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, Provider 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.	Use NCSR Maturity Scale
	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.	Use NCSR Maturity Scale

Function	Category	Contractor Response
	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.	Use NCSR Maturity Scale
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Use NCSR Maturity Scale
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Use NCSR Maturity Scale
	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.	Use NCSR Maturity Scale
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Use NCSR Maturity Scale

Function	Category	Contractor Response
	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.	Use NCSR Maturity Scale
	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.	Use NCSR Maturity Scale
	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.	Use NCSR Maturity Scale
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Use NCSR Maturity Scale
	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.	Use NCSR Maturity Scale
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Use NCSR Maturity Scale

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.	Use NCSR Maturity Scale
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Use NCSR Maturity Scale
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Use NCSR Maturity Scale
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (*e.g.*, external support from law enforcement agencies).	Use NCSR Maturity Scale
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Use NCSR Maturity Scale
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Use NCSR Maturity Scale
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Use NCSR Maturity Scale
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.	Use NCSR Maturity Scale

Function	Category	Contractor Response
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Use NCSR Maturity Scale
	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).	Use NCSR Maturity Scale