

# ATTACHMENT 1 - 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.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
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.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
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.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</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 EA.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
7	Describe your secure destruction practices and how certification will be provided to the EA.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	<a href="https://rschooldtoday.com/policies.html">https://rschooldtoday.com/policies.html</a>
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.

## ATTACHMENT 1(a) – 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
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> 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.	ID.AM-3
	<b>Business Environment (ID.BE):</b> 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.	ID.BE-4
	<b>Governance (ID.GV):</b> 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.	ID.GV-4
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-6
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1
	<b>Supply Chain Risk Management (ID.SC):</b> 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	ID.SC-4

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> 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.	PR.AC-7
	<b>Awareness and Training (PR.AT):</b> 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.	PR.AT-5
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-7
	<b>Information Protection Processes and Procedures (PR.IP):</b> 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.	PR.IP-12
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-2
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-5
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	DE.AR-5
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-8
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained	DW.DP-5

Function	Category	Contractor Response
	and tested to ensure awareness of anomalous events.	
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	<b>RS.RP-1</b>
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	<b>RS.CO-4</b>
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	<b>RS.AN-5</b>
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	<b>RS.MI-2</b>
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	<b>RS.IM-2</b>
<b>RECOVER (RC)</b>	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	<b>RC.RP-1</b>
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	<b>RC.IM-2</b>
	<b>Communications (RC.CO):</b> 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).	<b>RC.CO-3</b>