INSTRUCTIONS FOR COMPLETING FORM CPO2-2D

CONTRACTOR’S DATA PRIVACY AND SECURITY PLAN

The NIST Cybersecurity Framework Version 1.1 is the standard for data security and privacy for NYSED, and its related policies. Third party contractors that do business with NYSED must submit a plan that outlines how the contractor will align with the NIST CSF and implement all (i) state, (ii) federal, and (iii) NYSED data security and privacy contract requirements, over the life of the contract. We have created this template for contractors to use to submit the required data security and privacy plan.

The New York State Education Department (NYSED) 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.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
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.	
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.	

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 NYSED.	
6	Describe how data will be transitioned to the NYSED when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the NYSED.	
8	Outline how your data security and privacy program/practices align with NYSED's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	

The NIST CSF is the standard for educational agency data privacy and security policies and programs in NY. The table below will aid the review of a contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections to describe how their policies and practices align with the outlined controls/requirements in the Data Privacy and Security Plan template. To complete these sections, a Contractor may: (i) Use a narrative to explain alignment; (ii) Reference its applicable policies that align with outlined controls and attach such policies; and/or (iii) Explain why a specific control may not apply to the transaction contemplated. The informational references for each subcategory can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

NOTE:

Only the first page of this form is included in these instructions because the instructions appear at the top of the form.

NIST Cybersecurity Framework version 1.1			
Function	Category	Subcategory	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.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	
		ID.AM-2: Software platforms and applications within the organization are inventoried	
		ID.AM-3: Organizational communication and data flows are mapped	
		ID.AM-4: External information systems are catalogued	
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	

		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	
	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.	**ID.BE-1:** The organization’s role in the supply chain is identified and communicated	
		ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	
	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.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	

		ID.GV-4: Governance and risk management processes address cybersecurity risks	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	
		ID.RA-3: Threats, both internal and external, are identified and documented	
		ID.RA-4: Potential business impacts and likelihoods are identified	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	
		ID.RA-6: Risk responses are identified and prioritized	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	

	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.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	

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.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	
		PR.AC-2: Physical access to assets is managed and protected	
		PR.AC-3: Remote access is managed	
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	

	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.	**PR.AT-1:** All users are informed and trained	
		PR.AT-2: Privileged users understand their roles and responsibilities	
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	
		PR.AT-4: Senior executives understand their roles and responsibilities	
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	

	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.	**PR.DS-1:** Data-at-rest is protected	
		PR.DS-2: Data-in-transit is protected	
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	
		PR.DS-4: Adequate capacity to ensure availability is maintained	
		PR.DS-5: Protections against data leaks are implemented	
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	
		PR.DS-7: The development and testing environment(s) are separate from the production environment	
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	

	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.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	
		PR.IP-3: Configuration change control processes are in place	
		PR.IP-4: Backups of information are conducted, maintained, and tested	
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	
		PR.IP-6: Data is destroyed according to policy	
		PR.IP-7: Protection processes are improved	
		PR.IP-8: Effectiveness of protection technologies is shared	
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
		PR.IP-10: Response and recovery plans are tested	
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
		PR.IP-12: A vulnerability management plan is developed and implemented	

	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	
	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.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	
		PR.PT-2: Removable media is protected and its use restricted according to policy	
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	
		PR.PT-4: Communications and control networks are protected	
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	
		DE.AE-4: Impact of events is determined	
		DE.AE-5: Incident alert thresholds are established	

	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	
		DE.CM-4: Malicious code is detected	
		DE.CM-5: Unauthorized mobile code is detected	
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	
		DE.CM-8: Vulnerability scans are performed	

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	
		DE.DP-2: Detection activities comply with all applicable requirements	
		DE.DP-3: Detection processes are tested	
		DE.DP-4: Event detection information is communicated	
		DE.DP-5: Detection processes are continuously improved	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	

🟥	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	
		RS.CO-2: Incidents are reported consistent with established criteria	
		RS.CO-3: Information is shared consistent with response plans	
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	
		RS.AN-2: The impact of the incident is understood	
		RS.AN-3: Forensics are performed	
		RS.AN-4: Incidents are categorized consistent with response plans	
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	

	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	
		RS.MI-2: Incidents are mitigated	
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	
		RS.IM-2: Response strategies are updated	
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.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	
		RC.IM-2: Recovery strategies are updated	

🟩	**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).	**RC.CO-1:** Public relations are managed	
		RC.CO-2: Reputation is repaired after an incident	
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	

Additional Comments (If there is not enough room, additional pages can be attached):