

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The New York State Education Department (NYSED) requires all contracts with a contractor in which Confidential Information/Data will be provided to and/or accessible by the contractor include a Data Security and Privacy Plan. 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 Confidential Data/Information.	
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 Confidential Data/Information.	
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 Confidential Data/Information 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.	

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.

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	

<p>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.</p>	<p>ID.BE-1: The organization's role in the supply chain is identified and communicated</p>	
	<p>ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated</p>	
	<p>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated</p>	
	<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</p>	
	<p>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)</p>	
<p>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.</p>	<p>ID.GV-1: Organizational cybersecurity policy is established and communicated</p>	
	<p>ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners</p>	
	<p>ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p>	
	<p>ID.GV-4: Governance and risk management processes address cybersecurity risks</p>	

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

<p>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.</p>	<p>ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders</p>	
	<p>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</p>	
	<p>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.</p>	
	<p>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.</p>	
	<p>ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers</p>	

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)	

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

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

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

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

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	

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

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

<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>RS.CO-1: Personnel know their roles and order of operations when a response is needed</p>	
	<p>RS.CO-2: Incidents are reported consistent with established criteria</p>	
	<p>RS.CO-3: Information is shared consistent with response plans</p>	
	<p>RS.CO-4: Coordination with stakeholders occurs consistent with response plans</p>	
	<p>RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>	
<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>RS.AN-1: Notifications from detection systems are investigated</p>	
	<p>RS.AN-2: The impact of the incident is understood</p>	
	<p>RS.AN-3: Forensics are performed</p>	
	<p>RS.AN-4: Incidents are categorized consistent with response plans</p>	
	<p>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)</p>	

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

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

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