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.	All student and teacher data is stored in the Google Cloud Platform. Google Cloud firewalls are fully embedded in the cloud networking fabric. Passwords are hashed one way using the latest hashing algorithms. Google Cloud SQL Databases store all data which is encrypted during transfer using SHA-256 with RSA Encryption SSL Certificates.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	(See above)
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.	RocketLit restricts access to student and teacher data to only those staff members who require access for their job duties and require annual training for all employees.
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.	RocketLit Employees sign NDAs that cover data privacy restrictions in FERPA, COPPA, and Edlaw2D
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you	Within 72 hours of becoming aware of a privacy breach RocketLit will notify all impacted

	have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	parties. We use NJCIC as a notification system for our accounts and will receive notifications if our student PII has been breached.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon termination of this contract, RocketLit will give 60 days notice to the school district before removing all data from our system. if requested, will work within reasonable means to help the district to transfer information into a different system.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Elimination of student PII from our database and all relevant backups. Deletion of student PII from our database and all relevant backups.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	RocketLit Inc. uses the NIST framework to ensure that our privacy standards match the policies of the EA.
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.

EXHIBIT C.1 – 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.	**RocketLit inventories and documents our physical and digital assets, as well as documentation and data ownership through our NIST compliance document.**
	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.	**Through various teams and internal processes, we're constantly prioritizing, identifying and tuning our projects and risks, related to our business and users.**
	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.	**We've identified necessary trainings and systemic processes, such as background checks and maintain a list of classified risks to prioritize our operational and 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.	**Risk is assessed systematically through monthly meetings of our leadership team and new processes are applied to assess risk in various capacities.**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**We maintain an information security policy and have team members who explicitly manage the mitigation of risk.**
	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.	**As a virtual company, our supply chain risks are insignificant, but we've identified them and have a plan for managing them.**
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to	**Access to PII is strictly managed and only available in places where necessary for their function.**

Function	Category	Contractor Response
	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.	
	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.	**Training is conducted on a regular basis for all stakeholders that have access to PII and contribute to our overall cybersecurity.**
	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.	**We carefully manage all assets using industry standard practices.**
	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.	**Multiple internal documents are used to take stock of and manage processes and procedures related to protection and assets.**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**N/A**
	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.	**We use industry standard security measures to ensure compliance and data security.**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**We use multiple methods of tracking events and traffic for anomalous activity.**
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**Our assets are monitored internally via industry standard practices an externally through third parties.**
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**Testing and detection are maintained to ensure awareness.**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed	**Response planning is clarified and revisited annually.**

Function	Category	Contractor Response
	and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**Stakeholders for response have been identified and organized for any response that's needed.**
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**Analysis is ongoing to ensure response and recovery are expeditious.**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**Along with ongoing analysis, we're constantly undergoing mitigation efforts.**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**As organizational capacity grows, we add on additional structures to increase mitigation and response efficiency.**
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.	**Critical assets have processes in place for recovery.**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**As organizational capacity grows, we increase our ability to recover.**
	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).	**We've identified the critical parties for recovery and are prepared to assist in recovery efforts.**