BODDLE'S DATA PRIVACY AND SECURITY PLAN	
Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Over the duration of the contract, Boddle commits to implementing the relevant data security and privacy requirements by adopting a comprehensive, structured approach that is guided by the NIST Cybersecurity Framework. This will involve identifying and understanding the specific data security needs and risks, ensuring robust protection measures are in place, detecting any cybersecurity events promptly, responding effectively to any incidents, and recovering from any incidents to restore normal operations as quickly as possible. Additionally, Boddle will adhere to SOC 2 compliance requirements, which involve regular audits by external auditors to ensure that our data management practices meet the high standards for security, availability, processing integrity, confidentiality, and privacy of customer data. This will be reinforced through continuous monitoring and improvements to meet evolving threats and compliance requirements over the life of the contract. Our commitment to these frameworks ensures that data security and privacy are not one-time checks but are integral, ongoing processes throughout our engagement.
Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	To protect Personally Identifiable Information (PII), we have established a multi-layered security approach that includes the following measures: Administrative Safeguards: 1. Regular training sessions are conducted for all executive-level staff to ensure they are aware of cybersecurity best practices and compliance requirements. 2. Our Chief Technology Officer (CTO) oversees and ensures the implementation of all PII protection policies. Operational Safeguards: 1. We have a data disposal policy that dictates the secure deletion of digital assets containing PII, aligning with the specific requirements of the applicable school district. 2. Routine internal audits and reviews of our data protection practices are performed to ensure operational adherence to our security protocols. Technical Safeguards: 1. Network segmentation is managed by our CTO to isolate and secure servers containing sensitive information. 2. Multi-Factor Authentication (MFA) is mandatory for accessing financial accounts and crucial IT network accounts to prevent unauthorized access. 3. Encryption is applied to all data at rest to protect PII from potential breaches. 4. Data in transit is safeguarded through robust encryption protocols, ensuring PII is secure during transmission. 5. We employ advanced server-side systems to provide denial-of-service attack protection and continuous monitoring for malicious activities, ensuring that threats are detected and mitigated promptly. These safeguards are systematically reviewed and updated to adapt to emerging threats and to align with industry standards and regulatory requirements.
Address the training received by your	Our organization is committed to rigorous training programs to ensure that all employees and subcontractors with access to PII understand and adhere to the

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.	federal and state laws governing the confidentiality of Personally Identifiable Information (PII). This training is multifaceted and includes: 1. **Initial Training**: All new hires undergo mandatory training that covers the principles of data privacy, our internal data privacy policy, and the specific legal requirements for protecting PII under federal and state laws. This training includes practical scenarios and assessments to confirm understanding. 2. **Ongoing Education**: We hold regular meetings led by our IT leadership to update team members on any changes in data privacy laws and regulations. This ensures continuous awareness and compliance with evolving legal standards. 3. **Subcontractor Training**: Before beginning any work under the contract, subcontractors are required to complete a training program that mirrors the one for our own employees. 4. **Documented Acknowledgment**: Following training, all personnel, including subcontractors, must sign agreements affirming their understanding of and commitment to our internal data privacy policies and the legal obligations they are under. This comprehensive training framework is designed to instill a culture of privacy and security, ensuring that all parties involved in handling PII under the contract are knowledgeable and compliant with applicable confidentiality laws.
Specify if Processor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;	Our contracting processes are designed to ensure full compliance with the requirements of the Contract, particularly concerning the handling of PII. These processes include several key steps: 1. **Contractual Agreements**: At the onset of their engagement, all employees and subcontractors are required to sign a binding agreement that incorporates the Contract's terms, with explicit clauses relating to data privacy and the safeguarding of PII. 2. **Clause Specificity**: These agreements include detailed provisions that explicitly state the responsibilities and obligations in handling PII, adherence to our internal data privacy policies, and compliance with relevant federal and state laws. 3. **Verification of Understanding**: We verify that all signatories have read and understood the obligations through acknowledgment forms and, if necessary, through verbal confirmation during onboarding or training sessions.
Specify how the Processor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to	Our approach to managing data security and privacy incidents involving PII is anchored in a detailed Incident Response Plan (IRP). The IRP delineates a structured response strategy that consists of the following phases: 1. **Detection**: We deploy sophisticated monitoring tools and techniques to swiftly identify any potential breaches or unauthorized disclosures of PII. This system alerts our security team to anomalies that may indicate a security event. 2. **Assessment**: Upon detection, we conduct an immediate assessment to determine the scope and impact of the incident, categorizing it by severity and potential impact on stakeholders. 3. **Containment**: Our first priority is to contain the incident to prevent further unauthorized access or data loss. This includes temporary isolation of affected systems if necessary.

promptly notify NYC DOE;	4. **Eradication**: After containment, we work to remove the root cause of the incident and any related threats from our systems to prevent recurrence. 5. **Recovery**: We then restore and validate system functionality, ensuring that all systems return to normal operation securely and as quickly as possible. 6. **Lessons Learned**: After managing the incident, we conduct a thorough review to identify improvements to our security posture and incident handling processes. 7. **Reporting**: In the event of an incident, we have a protocol for promptly notifying users. This includes initial incident notification within an established timeframe, followed by periodic updates as more information becomes available and a comprehensive report after the incident has been resolved.
Describe whether, how and when data will be returned to the NYC DOE, transitioned to a successor contractor, at the NYC DOE's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.	When the data is no longer required to fulfill our contractual obligations, data will be destroyed and/or deidentified according to policy and within agreements with school customer users.

EXHIBIT C.1 – NIST CSF TABLE

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.	Boddle employs a systematic asset management process in line with ISO 27001's A.8 control category and NIST 800-53's asset management controls. This process ensures all assets are identified, classified, and managed according to their importance to our business objectives and risk strategy. Our Asset Management Policy, documented and reviewed annually, details the responsibilities for asset registration, classification, and handling, ensuring a comprehensive understanding and management of our data, personnel, devices, systems, and facilities.
	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.	Our Business Environment Management strategy, guided by ISO 27001's A.5 and NIST 800-53's PL-1 and RA-3 controls, ensures a deep understanding of the organization's mission, objectives, stakeholders, and activities. This strategic insight forms the basis for defining cybersecurity roles, responsibilities, and risk management decisions, ensuring they are closely aligned with our overarching business goals.
	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.	Governance at Boddle is structured around ISO 27001's A.5 control set and NIST 800-53's governance controls, ensuring comprehensive management of regulatory, legal, risk, environmental, and operational requirements. Our Governance Policy outlines how these elements inform cybersecurity risk management, ensuring alignment with best practices and compliance standards.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Risk assessments at Boddle are conducted in alignment with ISO 27001's A.12.2.1 and NIST 800-53's RA controls, providing a thorough understanding of the cybersecurity risks to our operations, assets, and individuals. This process informs our risk treatment plans and security measures, ensuring they are adequately prioritized and managed.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Our Risk Management Strategy integrates principles from ISO 27001's clause 6.1.1 and NIST 800-53's RM controls, establishing clear priorities, constraints, risk tolerances, and assumptions. This strategy supports our operational risk decisions and is documented in our Risk Management Policy.
	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.	Our supply chain risk management strategy aligns with ISO 27001's A.15.1.1 and NIST 800-53's SA-12 principles to identify, assess, and manage risks from third-party vendors and partners. We conduct thorough risk assessments of our supply chain, integrating these considerations into our overall risk management strategy to address potential vulnerabilities and threats from external sources. This is documented in our Third-Party Management Policy.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users,	In alignment with ISO 27001's A.9 and NIST 800-53's AC controls, we limit access to our assets based on authorization, need-to-know, and least privilege principles. Our Access Control Policy ensures consistent

Function	Category	Contractor Response
	processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	application of these controls across physical and logical domains.
	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.	Boddle's awareness and training programs are consistent with ISO 27001's A.7.2.2 and NIST 800-53's AT controls. These programs ensure that all personnel are aware of cybersecurity risks and understand their responsibilities, as documented in our Human Resource Security Policy.
	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.	Boddle's Data Security practices adhere to ISO 27001's A.8 and NIST 800-53's SC controls, ensuring the confidentiality, integrity, and availability of information. Our Data Management Policy covers data handling, encryption, and retention, aligning with our risk strategy to safeguard data throughout its lifecycle.
	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.	Our security policies, including purpose, scope, roles, responsibilities, and management commitment, are documented within our Information Security Policy Framework. This framework aligns with ISO 27001's A.5 and NIST 800-53's PM controls, ensuring a coordinated approach to protect information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Maintenance and repair of systems are performed in accordance with established policies and procedures. This approach ensures the continued security and resilience of our information systems.
	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.	Our organization employs technical security solutions to protect and ensure the resilience of our systems and assets. These solutions are managed in alignment with our policies, procedures, and ISO 27001's A.12 and NIST 800-53's PE and SC controls, safeguarding against potential cybersecurity threats.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	We have implemented systems and processes to detect anomalous activity and understand the potential impact of events. This capability ensures timely identification of potential security incidents.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Continuous monitoring at Boddle is performed in accordance with ISO 27001's A.16.1.7 and NIST 800-53's CM controls. Our Policy ensures that information systems and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes and procedures are maintained and regularly tested to ensure timely and effective awareness of anomalous events. This practice supports emphasis on continuous improvement and adaptability in the face of evolving cybersecurity threats.

Function	Category	Contractor Response
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	In alignment with ISO 27001's A.16 and NIST 800-53's IR controls, our incident response processes are documented in the Incident Response Plan. This plan is executed and maintained to ensure an organized and effective 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).	Response activities at Boddle are coordinated with internal and external stakeholders as outlined in our Incident Response Plan. This Plan is consistent with ISO 27001's A.16.1.5 and NIST 800-53's IR-4 control, ensuring effective communication during and after cybersecurity incidents.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Post-incident analysis is conducted to understand attack vectors, impacts, and effectiveness of response strategies. This analysis informs our continuous improvement process, aligning with information security approach to learning from incidents.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Our Mitigation Procedures are designed to prevent the expansion of events, mitigate their effects, and enable timely resolution. These procedures comply with ISO 27001's A.16.1.4 and NIST 800-53's IR controls, ensuring swift and effective incident mitigation.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Lessons learned from incident response activities are integrated back into our cybersecurity policies and processes, fostering a culture of continuous improvement.
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.	Our Incident Response Plan controls and outlines procedures to restore systems and assets affected by cybersecurity incidents. This plan is executed and maintained, ensuring efficient recovery and minimization of downtime.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery processes are regularly reviewed and improved, incorporating lessons learned from recovery activities and testing, consistent with ISO 27001's emphasis on continual improvement.
	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).	Communications during recovery activities are coordinated with relevant internal and external parties, ensuring transparency and alignment with ISO 27001's standards for effective communication.