Exhibit “A-1”

Education Law Section 2-d Contract Addendum

The parties to this Contract Addendum are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and Panorama Education ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law (“Section 2-d"), and Vendor may be considered a third party contractor, as that term is used in Section 2-d. BOCES and Vendor have entered into this Contract Addendum to conform to the requirements of Section 2-d and its implementing regulations as applicable. To the extent that any term of any other agreement or document conflicts with the terms of this Contract Addendum, the terms of this Contract Addendum shall apply and be given effect.

Definitions

As used in this Addendum and related documents, the following terms shall have the following meanings:

“Student Data" means personally identifiable information from student records that Vendor receives in connection with providing Services under this Agreement.

“Personally Identifiable Information” ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

“Third Party Contractor,” “Contractor" or “Vendor” means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

“BOCES” means Monroe #1 Board of Cooperative Educational Services.

“Parent” means a parent, legal guardian, or person in parental relation to a student.

“Student” means any person attending or seeking to enroll in an educational agency.

“Eligible Student” means a student eighteen years or older.

“State-protected Data” means Student Data, as applicable to Vendor’s product/service.

“Participating School District” means a public school district or board of cooperative educational services that obtains access to Vendor’s product/service through a cooperative educational services agreement (“CoSer”) with BOCES, or other entity that obtains access to Vendor’s product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor’s product/service to support its own educational programs or operations.

“Breach” means the unauthorized access, use, or disclosure of personally identifiable information or State-protected Data.

“Commercial or marketing purpose” means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students.

“Disclose”, “Disclosure,” and “Release” mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement;

(c) not disclose any personally identifiable information to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology as defined in Section 2-d;

(f) not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after such discovery of such breach;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information;

(i) adopt reasonable and appropriate technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, and that comply with the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the Data belongs to and is owned by the Participating School District from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may otherwise be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with the terms of this Addendum or the service order or its related exhibits the terms of this Contract Addendum first and then the service order (with Exhibits) shall be given precedence; and

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full cost of such legally required breach notification to parents and eligible students due to the unauthorized release of student data to the extent caused solely by Vendor or its agent or assignee failing to maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security
(https://www.monroe.edu/domain/1478)

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320. (https://www.monroe.edu/6320)
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing, to:

   Chief Privacy Officer
   New York State Education Department
   Room 863 EBA
   89 Washington Avenue
   Albany, New York 12234.

   or

   Monroe One Data Protection Officer
   William Gregory
   Monroe #1 BOCES
   41 O'Connor Road
   Fairport, NY 14450

Supplemental Information About Agreement Between Panorama Education and BOCES

(a) The exclusive purposes for which the personally identifiable information will be used by Vendor is to provide the related-based platform described in the Panorama service order and/or its related exhibits.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to materially consistent data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Agreement shall be from the effective date of the Panorama Education service order and it shall remain in effect until terminated by either party in accordance with the terms of the service order and its related exhibits.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, Vendor shall, upon written notice from BOCES, transfer all student data and protected principal and teacher data to the educational agency in a format agreed upon by the parties, or otherwise delete such data upon prior notice to BOCES where transfer is not technically feasible. Vendor shall thereafter securely delete in accordance with NIST 800-88r1 all student data and protected principal and teacher data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all student data and protected principal and teacher data maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the student data and protected principal and teacher data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities, except as required by applicable law or applicable regulations or to the extent data is retained in backups and archives, which shall be treated in accordance with Vendor's data retention schedules. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party except with BOCES' prior written consent. Upon written request, Vendor and/or its subcontractors or assignees will provide a written confirmation to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must reasonably cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will reasonably cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vender affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as Attachment 1 and is incorporated herein by reference as if fully set forth herein.

It is understood that a further Contract Addendum may be necessary to ensure compliance with Education Law Section 2-d and its implementing regulations, following promulgation by the New York State Education Department, and the parties agree to take such additional steps as may be necessary at that time.

Kelly Osborne

Vendor Signature

06 / 29 / 2023

Date

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.	Panorama uses CLM software to store contracts including any client specific requirements. Panorama is compliant with applicable laws on data privacy, and if there are any client-specific requirements, the contracts team has an internal escalation policy designed specifically for review, approval, and implementation of client requirements. If a client-specific requirement is approved, the requirement is noted in the CLM and implemented thereafter. Further, Panorama's legal team actively reviews state and local laws and informs the contracts team of any necessary updates.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Exhibit C.1. Panorama is fully compliant with the Family Educational Rights and Privacy Act (FERPA), the Pupil Privacy Protection Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and has signed the Student Privacy Pledge. Panorama Education uses a combination of Heroku and Amazon Web Services for hosting its systems, both of which are industry-leading cloud infrastructure services for web hosting and data processing. Specifically, Heroku and AWS services are continuously and rigorously tested against leading Cybersecurity frameworks, including SOC-2, ISO, HIPAA, and PCI DSS, among others. These assessments are conducted by independent evaluators and their findings are readily available on Heroku and AWS'

		websites. All Panorama data is hosted and processed in Amazon's us-east-1 region located in Virginia. Further, Panorama uses industry-standard practices for web application architecture, including encryption of data in-flight & at rest, HTTPS communication, and failover databases. Panorama limits its access to cloud systems only to engineers working directly on the platform. All employee access to cloud systems is gated behind single sign-on logins that are unique to each employee and require multi-factor authentication before granting access. When granted, access to cloud systems is ephemeral and expires after a few hours before requiring the employee to log in again. Panorama, in turn, employs teams of engineers dedicated to monitoring platform health and security. Engineering teams use leading cloud security posture tools and security event management systems provided by Heroku, Amazon, Datadog, Sentry, and New Relic to detect anomalous activity and protect against intrusions. Panorama maintains an incident response protocol that dictates how incidents are investigated and mitigated. Engineering teams run quarterly drills to test their familiarity with the protocol and to measure their response against incidents related to platform health and security. To validate the strength of Panorama's security posture, Panorama has partnered with Independent Security Evaluators ("ISE") to run penetration tests against platform systems. These tests evaluate the security of Panorama's website and infrastructure systems. On Panorama's website, ISE tests against front-end malicious tactics such as credential stuffing, cross-site scripting, and SQL injection. For platform infrastructure, ISE checks firewall configurations, database security, and internal access controls. Panorama's Security and Privacy programs are guided by publications from the National Institute of Standards and Technology ("NIST") standards. NIST publishes a framework of security activities and outcomes that a mature security program is expected to exhibit, including how internal access controls and

		infrastructure are managed. Panorama internally tracks its programs that are meeting these expectations. Moreover, Panorama has an appointed Trust Council of internal engineering, privacy, security, and legal resources that work alongside the Information Security team to rigorously evaluate, prioritize, and mitigate theoretical risks or gaps. To ensure Panorama's commitment to the NIST framework, Panorama partnered with Atredis as another vendor to periodically conduct interviews and assess Panorama's security program against the NIST Framework. Atredis has provided guidance and helped co-develop a long-term plan for Panorama's security and data privacy programs as the organization continues to develop. Panorama's security partners, ISE & Atredis, are able to provide executive summaries of their findings upon request. In addition, Panorama can provide infrastructure diagrams capturing any configurations being considered.
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.	Panorama conducts annual security and privacy training for all employees, during which among other things they are reminded of their obligation to protect 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.	Panorama's agreements with its subcontractors require them to adhere to all applicable laws regarding data privacy and contain terms that are at least as
		protective of EA's data as the ones contained in the Contract. Panorama's legal team and security team review new vendor agreements for consistency.

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.	Panorama maintains an incident response protocol that will be exercised in the event that a data incident is suspected. If Panorama experiences a breach or other incident that triggers the breach notification, Panorama will comply with applicable law(s) and follow the required steps for notification and mitigation. In the case of a reportable breach or equivalent reportable incident, regardless of whether experienced by Panorama or a customer, Panorama will provide the affected customer with information customer may use to respond to inquiries, such as: • What happened • What information was involved • What we are doing about it • What you can do for more information
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Panorama will coordinate with the EA via the EA's main point of contact in following the Contract's directions to transition and then subsequently delete the subject data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Panorama deletes electronic data in accordance with NIST 800-88 r1 at a level of sanitization that makes it impossible to recover data in the normal course of Panorama's data operations and renders it infeasible to recover any data from devices with ordinary techniques. To the extent Panorama identifies print materials in its possession that contain PII, it shreds such materials. Certification will be provided in writing as provided in the Contract.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Panorama follows the programs and practices that align with NIST's Cybersecurity Framework. See Exhibit C.1.

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

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.	Panorama Operations collects information related to all laptop assets. Information documented includes the date the asset was ordered and the make, model and serial number of the laptops, as well as user name for all other devices and systems, reliance is placed on the vendors that support Panorama's IT infrastructure. Panorama maintains a list of applications reviewed for use at Panorama as a related subsection associated with the information security policy. These applications have been reviewed by information Security. Additionally, Panorama maintains a listing of the applications that are approved for use with data classified as Tier 1 data. Panorama has deployed a software tool that will limit what software can be installed on Panorama issued laptops and will be able to provide a formal listing of software installed on laptops. Generally, the content of nearly all existing Panorama policies help inform employees of expectations related to organizational communication. As heavy reliance is placed on external vendors to provide infrastructure services that support Panorama services and products, there is good awareness of these vendors and these external information systems have been cataloged.
	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.	Panorama has a clear direction in the market and has clearly defined relationships with vendors and customers. Panorama's role is communicated with Panorama employees through the onboarding process and through quarterly goal setting. The majority of critical infrastructure necessary for Panorama is provided by third-parties. Documentation exists within Panorama's internal knowledgebase to help Panorama employees understand these relationships. The onboarding process as well as periodic training helps Panorama employees better understand the critical infrastructure.

	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.	Panorama has documented information security requirements and has made the policy available to Panorama employees within the company knowledgebase. Panorama has a cross-functional "Trust Council" responsible for identifying risks, implementing appropriate protocols and overseeing the company's privacy and security program. Panorama has documented information security requirements and has made the policy available to Panorama employees within the company knowledgebase. The company's security policies are applicable to all Panorama employees.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Panorama relies on vendors to identify and document asset vulnerabilities in critical infrastructure. Panorama deployed a tool which enforces set security settings on the laptops such as requirements for strong passwords and hard drive encryption. Personal phones used by Panorama employees are also required to have mobile device management software installed which forces the use of a PIN and the use of encryption. Members of Panorama's Trust Council are involved in information sharing forums and also receive notifications from vendors related to threat intelligence. Panorama has documented potential business impacts and likelihoods and third-party vendor risks.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Through the existing information security policy content and through onboarding activities, Panorama's risk tolerance is communicated. Critical infrastructure can be determined based on whether it is used to store and process Tier 1 data (data that contains student PII and educational records). Further, critical vendors have also been identified and are documented based on the same criteria.

	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.	Panorama vendors are clearly identified and effort is made to review contractual requirements to ensure that adequate availability and data protection requirements are in place. Critical third-party services that are used to store and process Tier 1 data have also been identified. Critical third-party vendors are onboarded with highly available services already configured. Where determined necessary, additional resiliency is acquired from these vendors. Close working relationships exist between Panorama team members and the vendors and recovery efforts are jointly made as issues arise.
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.	All Panorama employees are issued usernames and passwords in order to access information systems. Credentials are managed, verified, and revoked. Employees are responsible to maintain the physical security of their issued laptops. Requirements for physical security are documented within the information security policy. Employees are able to log into Panorama information systems remotely. All information systems containing Tier 1 data require two factor authentication. Panorama has developed role-based access which limits employees to the access required to perform their job responsibilities. Additionally, the information security policy contains a reference to minimum access necessary to Tier 1 data. Reliance on network integrity controls is placed on the vendors (i.e., AWS and Heroku) that provide infrastructure services. Identities of employees are effectively validated prior to the issuance of credentials.
	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.	All Panorama employees are trained during an onboarding session at the time of hire and then on an annual basis. Information security is one of the areas where training is provided. Privileged employees such as engineers receive additional instruction with role-specific onboarding. Requirements related to third-party stakeholders are formally documented within applicable contracts.

	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.	Panorama requires the encryption of all data at rest. Employees are issued laptops with disk encryption enabled. Employees that utilize their personal mobile phones to conduct business are required to install mobile device management software that forces encryption of data. Vendors providing infrastructure and platform services all encrypt data at rest. Panorama has provided guidance to employees on the appropriate methods for the secure exchange of Tier 1 data within the information security policy. Panorama manages laptops throughout the process of purchase, issuance, and retrieval. Assets are stored in a secured area within the office when not in the possession of an employee. All other supporting infrastructure assets are maintained and managed by critical vendors. Panorama maintains close relationships with their critical infrastructure vendors and places reliance on them to monitor for capacity
		constraints and to notify Panorama if additional resources need to be made available. Panorama has tools in place to generate alerts in data within Google drive when data is made accessible to non-Panorama entities. Reliance is also placed on infrastructure vendors to monitor for data leaks. Integrity checks related to software occur through the SDLC process. Employees are encouraged to download software only from reputable sources. A significant reliance is placed on critical infrastructure service providers to maintain information integrity processes. Panorama utilizes playground and staging environments separate from the production environment. All code is tested prior to being deployed in production. Panorama relies on its critical infrastructure service providers to validate hardware integrity and to resolve any issues.

	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.	Panorama relies on its critical infrastructure service providers to monitor baseline configurations and provide notifications related to unusual activity. Panorama follows an Agile process for code development. Peer review and code testing are standard practices and workflows ensure that required steps are followed. Panorama will open Jira tickets for some configuration changes such as the implementation of a new version of software. Tickets are used to document testing and to schedule the change. Panorama relies on its critical infrastructure vendor to perform regular backups of information. Restores of data are common and serve as a test of a backup process. Panorama relies on its critical infrastructure vendor to monitor the physical operating environment and to securely dispose of Panorama data. Additionally, Panorama employees are asked to destroy any Tier 1 data that temporarily needs to be stored on the employee's laptop hard drive.
		The Trust Council meets biweekly and regularly assesses data protection processes. The Trust Council shares the effectiveness of the protection technologies with stakeholders primarily through their participation in the incident management process. Vendors provide highly available platforms and failovers are regular, which also constitute business continuity tests. The incident response process is in place and facilitated by the Trust Council in conjunction with stakeholders. Criminal background checks are performed for all Panorama employees at the time of hire and annually thereafter. Panorama relies on its critical infrastructure vendors to monitor for and remediate

		vulnerabilities. Additionally, within the SDLC process tools are run to scan for vulnerabilities in code.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Panorama relies on its critical infrastructure vendors to maintain and repair assets that support Panorama products.
	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.	Audit logs are primarily maintained by the critical infrastructure vendors, but Panorama engineers are able to review logs as necessary to perform their responsibilities. Removable media is rarely used, however if it is required, media will be provided to Panorama employees. Removable media is not approved for storage of Tier 1 data. Panorama has implemented the principle of least privilege by assigning roles to employees which only provide them with the access needed to perform their responsibilities. Panorama relies on its critical infrastructure vendors to protect communications and networks and to provide load balancing across its services.

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Panorama relies on its critical infrastructure vendors to monitor network baselines and provide notifications for any unusual activities. The Trust Council facilitates the incident management process during which detected events are analyzed and categorized. Panorama relies on its critical infrastructure vendors to maintain audit logs. When the Panorama team is investigating incidents, event data is collected and correlated as necessary to perform their analysis. The Panorama team assesses the impact of the analyzed events, primarily by noting whether or not Tier 1 data was involved.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Panorama relies on its critical infrastructure vendors to monitor the network for security events and to provide notifications to Panorama related to any suspicious activity. Panorama relies on its critical infrastructure vendors to monitor the physical environment for security events and to provide notifications to Panorama related to any suspicious activity. Panorama relies on its critical infrastructure vendors to monitor network baselines and provide notifications for any unusual activities. Panorama relies on its critical infrastructure vendors to monitor for and remediate malicious code. Panorama relies on its critical infrastructure vendors to monitor for and remediate unauthorized mobile code. Panorama relies on its critical infrastructure vendors to perform vulnerability scanning of their environments.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection of events primarily occurs due to processing failures or customer complaints. There are roles and responsibilities associated with the individuals that observe these indicators and reach out to the Trust Council to initiate the incident management process. Panorama relies on its critical infrastructure vendors to provide notifications when unusual activity is found.

		Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	As necessary, response plans are documented and followed to recover from security incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Roles related to the incident management process are documented and are assigned to team members at the beginning of the investigation. Detection of events primarily occurs due to processing failures or customer complaints. There are roles and responsibilities associated with the individuals that observe these indicators and reach out to the Trust Council to initiate the incident management process. Response plans are developed as the incidents are investigated. If the incident involves Tier 1 data, the legal team and the PR team are notified and join the investigation. Information would be shared with customers and other external parties as needed.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Detection of events primarily occurs due to processing failures or customer complaints. There are roles and responsibilities associated with the individuals that observe these indicators and reach out to the Trust Council to initiate the incident management process. Impact associated with the incident is determined primarily on whether or not Tier 1 data was involved. Incidents are categorized primarily by whether or not Tier 1 data was involved. The organization as a whole is trained to understand the critical nature of protecting Tier 1 data. The individuals assigned to investigate identified incidents perform basic forensics such as log correlation and analysis. If additional forensics need to be performed, the team would involve experts as necessary.

PANORAMA EDUCATION - SERVICE ORDER

Primary Contact Information

Client		Panorama Education, Inc. ("Panorama")	
Client Legal Name ("Client")	Monroe 1 BOCES	*Company Name*	Panorama Education, Inc.
Primary Contact, Title	Cathy Hauber Ed.D, Assistant Superintendent for Instructional Programs	*Contact*	Account Management Team
Billing / Payment Address	41 O'Connor Rd	*Billing Address*	24 School St. Fourth Floor
City / State / Zip	Fairport, NY 14450	*City / State / Zip*	Boston, MA 02108
Primary Contact Email Address	cathleen_hauber@boces.monroe.edu	*Email*	Contact@panoramaed.com
Primary Contact Phone Number	585 383 2200	*Phone*	(617) 356-8123
Accounts Payable Contact	Karen Pitoni		
Accounts Payable Email Address	Karen_Pitoni@boces.monroe.edu		
Accounts Payable Phone Number	(585) 383-2263		
Purchase Order Required?	Yes [X] No [ ]		

(1) Description of Services and (2) Fees

Description of Services	Fees	
<u>Annual Licenses:</u> All licenses include access to Platform and Support (as defined in the Terms and Conditions): Survey administration, analysis and reporting. • Dashboards and reporting for teachers, student support staff, school administrators, and district administrators • Ongoing Project Management and Technical support through the length of the contract **Panorama Survey Platform** • Student Surveys • Teacher & Staff Surveys • Family Surveys	***Effective Date:***	09/08/2023
	Contract Term: *(From Effective Date)*	<u>09/08/2023 - 09/07/2024</u>
	Annual License Fee:	$6,500 / year
	Subtotal License Fee Over Contract Term:	$6,500
	Annual Total: *(Invoiced on Effective Date)*	$6,500 / year
	Total Over Contract Term:	$6,500

		The Trust Council is involved in forums where they are able to keep updated on new vulnerabilities. Additionally, a close relationship is maintained with critical infrastructure service vendors who also help Panorama become aware of new vulnerabilities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	When the Panorama team is investigating incidents, activities will be coordinated across the team members and/or vendors to contain and mitigate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.
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.	As necessary, recovery plans are documented and followed to recover from security incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.
	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).	Panorama has processes in place to communicate with customers in the event of an outage. If a significant breach were to occur, Panorama's executive team members and legal team would ensure proper reporting, communication and coordination. Panorama's security team would be responsible for repair and restoration activities, including coordinating with critical infrastructure vendors.

		The Trust Council is involved in forums where they are able to keep updated on new vulnerabilities. Additionally, a close relationship is maintained with critical infrastructure service vendors who also help Panorama become aware of new vulnerabilities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	When the Panorama team is investigating incidents, activities will be coordinated across the team members and/or vendors to contain and mitigate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.
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.	As necessary, recovery plans are documented and followed to recover from security incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Panorama performs a root cause analysis for all investigated incidents and works to make improvements to existing processes.
	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).	Panorama has processes in place to communicate with customers in the event of an outage. If a significant breach were to occur, Panorama's executive team members and legal team would ensure proper reporting, communication and coordination. Panorama's security team would be responsible for repair and restoration activities, including coordinating with critical infrastructure vendors.