PANORAMA EDUCATION - SERVICE ORDER

PANORAMA EDUCATION

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

1

PANORAMA EDUCATION - SERVICE ORDER

PANORAMA EDUCATION

(3) Agreement

The entire agreement by and between Client and Panorama ("Agreement") consists of (i) the terms set forth in this Service Order ("SO"); (ii) the terms attached as Exhibit A to, and hereby incorporated by reference into, this SO ("Terms"); and (iii) Education Law Section 2-d Contract Addendum between Client and Panorama attached as Exhibit A-1 to, and hereby incorporated by reference into, this SO.

(4) Supplemental Terms and Conditions (if any)

Authorization

By signing below, Client and Panorama ACCEPT AND AGREE TO the Agreement as of the Effective Date.

Client Signature:	Print Name, Title:	Date:
Panorama Signature: *Kelly Osborne*	Print Name, Title: Kelly Osborne, Contract Administrator	Date: 06 / 29 / 2023

2

BACKGROUND

Panorama is an education technology company that provides a cloud-based platform-as-a-service and related support services to enable schools and school districts to analyze student and school data, measure social-emotional learning, and design and implement survey programs for students, staff and parents or authorized guardians ("Platform"). The client named on the Service Order attached hereto ("Client") and Panorama have entered into an agreement consisting of the attached Service Order, including any exhibits attached thereto, ("SO"), these terms ("Terms" and collectively with the SO, "Agreement"). From time to time hereafter, Client and Panorama may enter into additional service orders pursuant to which Client may purchase additional rights to use the Platform and receive additional services, provided that these Terms will be incorporated by reference into and apply to each such additional service order to create a separate agreement that governs each such additional service order, in each case to the exclusion of any other terms or conditions that either party seeks to impose or incorporate or that are implied by course of dealing.

1 RIGHT TO USE PLATFORM

1.1 Platform. Subject to this Agreement, Panorama hereby grants Client (including Client's students, employees, and parents and authorized guardians of Client's students, all as applicable and described in the relevant SO, ("Authorized Users")), the limited, nonexclusive, nontransferable, non-sublicenseable right to access and use the Platform via the Internet during the Term solely for Client's use, in accordance with applicable laws and regulations and the Platform's intended uses as communicated to Client by Panorama.

1.2 Limitations. Except as expressly permitted in the Agreement, Client will not and will not authorize or allow any third party to: (a) provide access to the Platform to any person who is not an Authorized User or (b) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the Platform; (c) modify, translate or create derivative works based on the Platform; (d) copy, rent, lease, distribute, pledge, assign or otherwise transfer or allow any lien, security interest or other encumbrance on the Platform; (e) use the Platform for timesharing or service bureau purposes ; (f) hack, manipulate, interfere with or disrupt the integrity or performance of or otherwise attempt to gain unauthorized access to the Platform or its related systems, hardware or networks or any content or technology incorporated in any of the foregoing; or (g) remove or obscure any proprietary notices or labels of Panorama or its suppliers on the Platform or on any printed or digital materials provided by Panorama.

1.3 Compliance with Laws. Panorama is responsible for compliance with federal, state local laws and regulations to the extent they govern Panorama's activities, including providing the Platform to Client. Client is responsible for compliance with federal, state and local laws and regulations to the extent they govern Client's activities, including but not limited to the use by Client of the Platform to collect, record, retain, use and disclose any individual's information. Without limiting the foregoing, each party is responsible for determining its own obligations, including but not limited to notice and consent obligations, under the Family Educational Right to Privacy Act and its implementing regulations ("FERPA") and the Protection of Pupil Rights Act and its implementing regulations ("PPRA"). The parties agree that they intend for the collection and use of personally identifiable information (as defined under FERPA) for only legitimate educational purposes and other purposes allowed under relevant laws, including but not limited to FERPA, PPRA and New York Education Law Section 2-d. An Education Law Section 2-d Contract Addendum is attached hereto as Exhibit A-1 and is incorporated herein by reference as if fully set forth herein. Client hereby gives its consent to Panorama to the extent authorized by law on behalf of parents (as defined under FERPA, PPRA and the Children's Online Privacy Protection Act ("COPPA")) of children from whom any personal information (as defined under COPPA) may be gathered in connection with this Agreement and the Platform. Panorama shall not be obligated to obtain consents from parents directly.

2 INTELLECTUAL PROPERTY; PRIVACY; SECURITY

2.1 Client Data. As between Client and Panorama, Client owns data input into the Platform, or otherwise provided to Panorama, by Client and Authorized Users, that constitutes personally identifiable information (as defined under FERPA), such as student survey responses reported on an individual level, ("Client PII") and (b) any other data and content input into the Platform, or otherwise provided to Panorama, by Client and Authorized Users or on their behalf, such as survey questions, ("Non-PII" and together with PII "Client Data"). Client hereby grants Panorama a nonexclusive, worldwide, royalty-free, fully paid up, sublicenseable (through multiple tiers): (i) right and license during the Term to copy, distribute, display, create derivative works of and use Client Data only to perform Panorama's obligations under this Agreement; (ii) perpetual, irrevocable right and license to copy, modify and use Client PII to create aggregated, non-personally identifiable data sets ("Blind Data") and copy, distribute, display, create derivative works of and use only Blind Data for benchmarking, research or development purposes, including published research; and (iii) perpetual, irrevocable right and license to copy, distribute, display, create derivative works of and use de-identified Non-PII, for any and all purposes, in any form, media or manner. Client reserves any and all right, title and interest in and to Client Data other than the licenses therein expressly granted to Panorama under this Agreement.

2.2 Panorama Intellectual Property. Panorama retains all right, title and interest in and to the Platform, including but not limited to learning content, teaching materials, survey questions, underlying research and methodologies (by whomever produced except to the extent Client produced such material), all copies and parts of any of the foregoing, and all intellectual property rights therein. Panorama grants no, and reserves any and all, rights other than the rights expressly granted to Client under this Agreement with respect to the Platform.

3

2.3 <u>Client Feedback.</u> Client may from time to time provide suggestions, comments for enhancements or functionality or other feedback ("<u>Feedback</u>") to Panorama with respect to the Platform. Panorama has full discretion to determine whether to proceed with development of the requested enhancements, features or functionality. Client hereby grants Panorama a royalty-free, fully paid-up, worldwide, transferable, sublicenseable, irrevocable, perpetual license to: (a) copy, distribute, transmit, display, perform, and create derivative works of the Feedback in whole or in part; and (b) use the Feedback in whole or in part, including without limitation, the right to develop, manufacture, have manufactured, market, promote, sell, have sold, offer for sale, have offered for sale, import, have imported, rent, provide and lease products or services that practice or embody, or are configured for use in practicing, the Feedback in whole or in part.

2.4 <u>Panorama Privacy Policy</u>. Panorama's Privacy Statement, as may be amended from time to time, is available at https://www.panoramaed.com/privacy.

2.5 <u>Data Security and Privacy</u>.

(a) Panorama will implement and maintain an information security program that is consistent with industry recognized practices, which include using commercially reasonable administrative, physical and technical safeguards designed to protect the Platform from unauthorized access that could compromise the security, confidentiality or integrity of Client PII. Panorama shall: (i) use reasonable efforts to secure physical premises where Client PII will be processed and/or stored and (ii) take reasonable precautions with respect to the employment of, access given to, and education and training of personnel engaged by Panorama to perform its obligations under this Agreement.

(b) Client will and will instruct its Authorized Users to: (i) use the Platform to collect, record, retain, use and disclose personally identifiable information only to the extent necessary for its legitimate educational purposes; (ii) otherwise provide Panorama with personally identifiable information only to the extent necessary for Panorama to provide the Platform and perform its obligations under the Agreement; (iii) input personally identifiable information into the Platform only as prescribed by Panorama and only in the fields designated by Panorama ("<u>Structured Fields</u>"); (iv) use reasonable efforts to prevent unauthorized access to or use of the Platform; and (v) notify Panorama promptly of any known or suspected unauthorized access or use. Client will assist Panorama in all efforts to investigate and mitigate the effects of any such incident.

(c) If during the Term or upon termination of this Agreement Client requests in writing, Panorama will delete or otherwise render unrecoverable Client PII in Panorama's possession in a manner consistent with media sanitization practices described under industry recognized standards.

(d) Panorama shall not be responsible for any personally identifiable information input into the Platform in a manner not prescribed by Panorama or in a field that is not a Structured Field except as otherwise required by law.

3   FEES; PAYMENT TERMS

3.1 <u>Fees; Payment Terms</u>. Unless otherwise indicated on the SO, Client will pay all fees within thirty (30) days of the invoice date. If payment of any fee is not made when due and payable, a late fee will accrue at the rate of the lesser of one and one-half percent (1.5%) per month or the highest legal rate permitted by law and Client will pay all reasonable expenses of collection. In addition, if any past due payment has not been received by Panorama within thirty (30) days from the time such payment is due, Panorama may upon written notice to Client suspend access to the Platform until such payment is made.

3.2 <u>Taxes; Tax Exemption</u>. All amounts payable by Client to Panorama hereunder are exclusive of any sales, use and other taxes or duties, however designated, including without limitation, withholding taxes, royalties, know-how payments, customs, privilege, excise, sales, use, value-added and property taxes (collectively "<u>Taxes</u>"). To the extent applicable, Client will be solely responsible for payment of all Taxes and will not withhold any Taxes from any amounts due Panorama. For the avoidance of doubt, Taxes do not include taxes based on Panorama's income. Client is responsible for determining whether it qualifies for any tax exemption, and if Client claims it is tax-exempt, it will, upon request from Panorama, provide documentation evidencing its tax-exempt status.

4   TERM, TERMINATION

4.1 <u>Term</u>. The term of the Agreement will commence on the Effective Date and, unless earlier terminated in accordance with this Section 4, will continue through the date set forth on the SO ("<u>Term</u>").

4.2 <u>Expiration; Termination</u>. In addition to any other remedies it may have, either party may terminate the Agreement prior to expiration at any time and for any reason upon ninety (90) days' written notice to the other party. Upon expiration or any termination for any reason of the Agreement: (a) Client will pay in full for use of the Platform up to and including the last day on which the Platform is provided; (b) Panorama may, without notice to Client, delete or otherwise render unrecoverable Client PII in Panorama's possession in a manner consistent with legal requirements and media sanitization practices described under industry recognized standards; and (c) all rights granted to Client and all obligations of Panorama will immediately terminate and Client will promptly cease use of the Platform.

4.3 <u>Survival</u>. Upon expiration or termination for any reason of the Agreement, Sections 2 (Intellectual Property; Privacy; Security), 3 (Fees; Payment Terms), 4.2 (Termination; Effect of Termination), 4.3 (Survival), 5 (Confidentiality), 6.2 (Disclaimer), 7 (Limitations of Liability; Indemnification), and 8 (General) will survive.

5   CONFIDENTIALITY

5.1 As used herein, "<u>Confidential Information</u>" means, subject to the exceptions set forth in the following sentence, any

information or data that is not Client PII, regardless of whether it is in tangible form, disclosed by either party ("Disclosing Party") that Disclosing Party has either marked as confidential or proprietary, or has identified in writing as confidential or proprietary within thirty (30) days of disclosure to the other party ("Receiving Party"); provided, however, that a Disclosing Party's business plans, strategies, technology, research and development, current and prospective clients and customers, billing records, and products or services will be deemed Confidential Information of Disclosing Party even if not so marked or identified. Panorama's Confidential Information includes, without limitation, the Platform and this Agreement. Information will not be deemed Confidential Information" if such information: (a) is known to the Receiving Party prior to receipt from Disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to Disclosing Party; (b) becomes known (independently of disclosure by Disclosing Party) to the Receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to Disclosing Party; or (c) becomes publicly known or otherwise ceases to be secret or confidential, except through a breach of this Agreement by the Receiving Party. Each party acknowledges that certain Confidential Information may constitute valuable trade secrets and proprietary information of a party, and each party agrees that it will use the Confidential Information of the other party solely in accordance with the provisions of this Agreement and will not disclose, or permit to be disclosed, the same directly or indirectly, to any third party without the other party's prior written consent, except as otherwise permitted hereunder. Each party will use reasonable measures to protect the confidentiality and value of the other party's Confidential Information. Notwithstanding any provision of this Agreement, either party may disclose the terms of the Agreement, in whole or in part (i) to its employees, officers, directors, professional advisers (e.g., attorneys, auditors, financial advisors, accountants and other professional representatives), existing and prospective investors or acquirers contemplating a potential investment in or acquisition of a party, sources of debt financing, acquirers and/or subcontractors who have a need to know and are legally bound to keep such Confidential Information confidential by confidentiality obligations or, in the case of professional advisors, are bound by ethical duties to keep such Confidential Information confidential consistent with the terms of this Agreement; and (ii) as reasonably deemed by a party to be required by law (in which case each party will provide the other with prior written notification thereof, will provide such party with the opportunity to contest such disclosure, and will use its reasonable efforts to minimize such disclosure to the extent permitted by applicable law). Each party agrees to exercise due care in protecting the Confidential Information from unauthorized use and disclosure. In the event of actual or threatened breach of the provisions of this Section, the non-breaching party will be entitled to seek immediate injunctive and other equitable relief, without waiving any other rights or remedies available to it. Each party will promptly notify the other in writing if it becomes aware of any violations of the confidentiality obligations set forth in the Agreement. Upon Disclosing Party's written request, Receiving Party will either promptly return to Disclosing Party Disclosing

Party's Confidential Information, and all embodiments thereof, that is in Receiving Party's possession and certify such return or use reasonable efforts to delete or otherwise render inaccessible such Confidential Information and certify the same. The parties understand and agree that this Agreement will be approved by Client's Board of Education in public session and that this Agreement and its related documents and exhibits will be available on client's website and/or upon request, in accordance with the New York Public Officers Law and Education Law Section 2-d.

6   REPRESENTATIONS,   WARRANTIES   AND DISCLAIMER

6.1   Representations and Warranties.   Each party represents and warrants to the other party that (a) such party has the required power and authority to enter into this Agreement and to perform its obligations hereunder, (b) the execution of this Agreement and performance of its obligations thereunder do not and will not violate any other agreement to which it is a party or any law or regulation applicable to it, and (c) this Agreement constitutes a legal, valid and binding obligation when signed by both parties.   Client further represents and warrants that it has the right to provide Client Data to Panorama as well as the licenses and rights therein and thereto for the purposes contemplated by this Agreement.

6.2   Disclaimer.   EXCEPT AS EXPRESSLY SET FORTH HEREIN, THE PLATFORM IS PROVIDED ON AN "AS-IS" BASIS AND PANORAMA DISCLAIMS ANY AND ALL WARRANTIES. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS AGREEMENT, NEITHER PARTY MAKES ANY ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER. ALL   OTHER   EXPRESS   OR   IMPLIED   CONDITIONS, REPRESENTATIONS   AND   WARRANTIES   ARE   HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. EACH   PARTY   EXPRESSLY   DISCLAIMS   ALL   IMPLIED WARRANTIES   OF   MERCHANTABILITY,   FITNESS   FOR   A PARTICULAR PURPOSE, QUALITY, ACCURACY, TITLE, AND NON-INFRINGEMENT. NEITHER PARTY WARRANTS AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE PRODUCTS OR SERVICES   PROVIDED   BY   SUCH   PARTY   OR   AGAINST INFRINGEMENT.   NEITHER PARTY WARRANTS THAT THE PRODUCTS OR SERVICES PROVIDED BY SUCH PARTY ARE ERROR-FREE   OR   THAT   OPERATION   OF   SUCH   PARTY'S PRODUCTS   OR   SERVICES   WILL   BE   SECURE   OR UNINTERRUPTED. NEITHER PARTY WILL HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF THE OTHER PARTY TO ANY THIRD PARTY.

7   LIMITATIONS   OF   LIABILITY; INDEMNIFICATION

7.1   Disclaimer of Consequential Damages. THE PARTIES HERETO AGREE THAT, NOTWITHSTANDING ANY OTHER PROVISION IN THIS AGREEMENT, EXCEPT FOR LIABILITY ARISING OUT OF (A) USE OF THE PLATFORM OTHER THAN EXPRESSLY PERMITTED BY SECTION 1 (RIGHT TO USE PLATFORM), (B) EITHER PARTY'S BREACH OF SECTION 5

5

(CONFIDENTIALITY), (C) PANORAMA'S NOTIFICATION OBLIGATIONS AS SET FORTH UNDER NEW YORK EDUCATION LAW SECTION 2-D; AND (D) A PARTY'S INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 7.4 AND 7.5 BELOW, AS APPLICABLE, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, LOST OR DAMAGED DATA, LOST PROFITS OR LOST REVENUE, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF A PARTY HAS BEEN NOTIFIED OF THE POSSIBILITY THEREOF.

7.2   General Cap on Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, EXCEPT FOR LIABILITY ARISING OUT OF (A) CLIENT'S USE OF THE PLATFORM OTHER THAN EXPRESSLY PERMITTED BY SECTION 1 (RIGHT TO USE PLATFORM), (B) EITHER PARTY'S BREACH OF SECTION 5 (CONFIDENTIALITY), (C) PANORAMA'S NOTIFICATION OBLIGATIONS AS SET FORTH UNDER NEW YORK EDUCATION LAW SECTION 2-D;AND (D) A PARTY'S INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 7.4 AND 7.5 BELOW, AS APPLICABLE, UNDER NO CIRCUMSTANCES WILL EITHER PARTY'S LIABILITY FOR ALL CLAIMS ARISING UNDER OR RELATING TO THIS AGREEMENT (INCLUDING BUT NOT LIMITED TO WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED THE AGGREGATE FEES PAID BY CLIENT TO PANORAMA UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT OR CIRCUMSTANCES GIVING RISE TO SUCH LIABILITY. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT.

7.3   Independent Allocations of Risk. EACH PROVISION OF THIS AGREEMENT THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES IS TO ALLOCATE THE RISKS OF THIS AGREEMENT BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THIS AGREEMENT, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THEY HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

7.4   Indemnification by Panorama. Except for liability for which Client is responsible under Section 7.5, Panorama will indemnify, defend and hold Client and the officers, directors, agents, and employees of Client ("Client Indemnified Parties") harmless from settlement amounts and damages, liabilities, penalties, costs and expenses ("Liabilities") that are payable to any third party or incurred by the Client Indemnified Parties (including reasonable attorneys' fees) arising from any third party claim, demand or allegation that Panorama engaged in tortious conduct resulting in personal injury or tangible property damage and/or gross negligence and/or the use of the Platform in accordance with the terms and conditions of this Agreement infringes such third party's copyright or results in a misappropriation of such third party's trade secrets. Panorama will have no liability or obligation under this Section 7.4 if such

Liability is caused in whole or in part by (a) modification of the Platform by any party other than Panorama without Panorama's express consent; (b) the combination, operation, or use of the Platform with other product(s), data or services not provided by Panorama where the Platform would not by itself be infringing; or (c) unauthorized or improper use of the Platform. If the use of the Platform by Client has become, or in Panorama's opinion is likely to become, the subject of any claim of infringement, Panorama may at its option and expense (i) procure for Client the right to continue using the Platform as set forth hereunder; (ii) replace or modify the Platform to make it non-infringing so long as the Platform has at least equivalent functionality; (iii) substitute an equivalent for the Platform or (iv) if options (i)-(iii) are not available on commercially reasonable terms, terminate the Agreement. This Section 7.4 states Panorama's entire obligation and Client's sole remedies in connection with any claim regarding the intellectual property rights of any third party.

7.5   Indemnification by Client. Client will indemnify, defend and hold Panorama and the officers, directors, agents, and employees of Panorama ("Panorama Indemnified Parties") harmless from Liabilities that are payable to any third party or incurred by the Panorama Indemnified Parties (including reasonable attorneys' fees) arising from any third party claim, demand or allegation arising from or related to any use by Client or Authorized Users of the Platform or Client Data in violation of the Agreement or any applicable federal, state or local law or regulation.

7.6   Indemnification Procedure. If a Client Indemnified Party or a Panorama Indemnified Party (each, an "Indemnified Party") becomes aware of any matter it believes it should be indemnified under Section 7.4 or Section 7.5, as applicable, involving any claim, action, suit, investigation, arbitration or other proceeding against the Indemnified Party by any third party (each an "Action"), the Indemnified Party will give the other party ("Indemnifying Party") prompt written notice of such Action. Indemnified Party will cooperate, at the expense of Indemnifying Party, with Indemnifying Party and its counsel in the defense and Indemnified Party will have the right to participate fully, at its own expense, in the defense of such Action with counsel of its own choosing. Any compromise or settlement of an Action will require the prior written consent of both parties hereunder, such consent not to be unreasonably withheld or delayed.

8   GENERAL

8.1   International. Client may not remove or export from, or use from outside, the United States or allow the export or re-export of the Platform or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority.

8.2   Relationship. No agency, partnership, joint venture, or employment is created as a result of the Agreement and a party

6

does not have any authority of any kind to bind the other party in any respect whatsoever.

8.3   Publicity. Each party agrees that it will not, without prior written consent of the other, issue a press release regarding their business relationship. Notwithstanding anything herein to the contrary, Panorama may identify Client and the relationship between Panorama and Client in Panorama's marketing collateral, website, and other promotional, proposal and marketing materials.

8.4   Assignment. Neither party may assign the Agreement by operation of law or otherwise or assign or delegate its rights or obligations under the Agreement without the other party's prior written consent; provided however, that either party may assign the Agreement to an acquirer of or successor to all or substantially all of its business or assets to which the Agreement relates, whether by merger, sale of assets, sale of stock, reorganization or otherwise. Any assignment or attempted assignment by either party otherwise than in accordance with this Section 8 will be null and void.

8.5   Equitable Relief. In any action or proceeding to enforce rights under the Agreement, the prevailing party will be entitled to recover costs and attorneys' fees. Client acknowledges that any unauthorized use of the Platform will cause irreparable harm and injury to Panorama for which there is no adequate remedy at law. In addition to all other remedies available under the Agreement, at law or in equity, Client further agrees that Panorama will be entitled to injunctive relief in the event Client uses the Platform in violation of the limited license granted herein or uses the Platform in any way not expressly permitted by the Agreement.

8.6   Force Majeure. Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service, in whole or in part, as a result of a cause beyond its reasonable control and without its fault or negligence, including, but not limited to, acts of God, acts of war, epidemics, fire, communication line failures, power failures, earthquakes, floods, blizzard, or other natural disasters (but excluding failure caused by a party's financial condition or any internal labor problems (including strikes, lockouts, work stoppages or slowdowns, or the threat thereof)) ("Force Majeure Event"). Delays in performing obligations due to a Force Majeure Event will automatically extend the deadline for performing such obligations for a period equal to the duration of such Force Majeure Event. Except as otherwise agreed upon by the parties in writing, in the event such non-performance continues for a period of thirty (30) days or more, either party may terminate the Agreement by giving written notice thereof to the other party. Upon the occurrence of any Force Majeure Event, the affected party will give the other party written notice thereof as soon as reasonably practicable of its failure of performance, describing the cause and effect of such failure, and the anticipated duration of its inability to perform.

8.7   Governance. This Agreement will be governed by the laws of the state of New York without regard to its conflict of laws provisions. For all disputes relating to this Agreement, each party submits to the exclusive jurisdiction of the state and federal courts located in Monroe County, New York and waives any jurisdictional, venue, or inconvenient forum objections to such courts.

8.8   Agreement. Both parties agree that the Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of the Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein. If any provision of the Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that the Agreement will otherwise remain in full force and effect and enforceable. Any additional or different terms proposed by Client, including those contained in Client's procurement order, acceptance, vendor portal or website, shall not be valid or have any effect unless expressly incorporated into the SO and agreed upon in writing by Panorama. Neither Panorama's acceptance of Client's procurement order nor its failure to object elsewhere to any provisions of any subsequent document, website, communication or act of Client shall be deemed acceptance thereof or a waiver of any of the terms in these Terms. If any term of the SO, including any exhibit attached thereto, expressly conflicts with a term of these Terms, the term of the SO (or if applicable the exhibit) shall prevail. If terms within the SO, including any exhibit attached thereto, and these Terms appear merely inconsistent or ambiguous, all such terms shall be given effect to the extent reasonably possible, with a term that is more specific and detailed on a certain matter prevailing over a more general term or silence on that matter. Silence in the SO, or in any exhibit attached thereto, or in these Terms, on a matter that is addressed elsewhere in the Agreement shall not be deemed to present an express conflict, inconsistency or ambiguity.

8.9   Notices. All notices under the Agreement will be in writing and sent to the recipient's address set forth in the SO and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

7

Title	Monroe 1 BOCES Agreement
File name	Monroe 1 BOCES (N...023 Final GeM.pdf
Document ID	d88d9933948b10225fbbf854a5c2c342a0402d2a
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

⬈ SENT	**06 / 29 / 2023** 18:47:59 UTC	Sent for signature to Panorama Finance Team (contracts@panoramaed.com) from tpetruzziello@panoramaed.com IP: 173.71.94.134
◉ VIEWED	**06 / 29 / 2023** 18:56:11 UTC	Viewed by Panorama Finance Team (contracts@panoramaed.com) IP: 38.92.35.189
ⱽ SIGNED	**06 / 29 / 2023** 18:58:30 UTC	Signed by Panorama Finance Team (contracts@panoramaed.com) IP: 38.92.35.189
✓ COMPLETED	**06 / 29 / 2023** 18:58:30 UTC	The document has been completed.

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.

<u>Definitions</u>

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

(I)   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

Title	Monroe 1 BOCES Agreement 2
File name	Monroe.1.BOCES (N...8-2023 Final .pdf
Document ID	51dee571308c52f552346b5868425c323e1ed7eb
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

⤴ **SENT**	**06 / 29 / 2023** 18:49:07 UTC	Sent for signature to Panorama Finance Team (contracts@panoramaed.com) from tpetruzziello@panoramaed.com IP: 173.71.94.134
◎ **VIEWED**	**06 / 29 / 2023** 18:58:40 UTC	Viewed by Panorama Finance Team (contracts@panoramaed.com) IP: 38.92.35.189
〆 **SIGNED**	**06 / 29 / 2023** 18:59:07 UTC	Signed by Panorama Finance Team (contracts@panoramaed.com) IP: 38.92.35.189
⊘ **COMPLETED**	**06 / 29 / 2023** 18:59:07 UTC	The document has been completed.

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

PANORAMA EDUCATION

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	
Annual Licenses: 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		***Effective Date:***	09/08/2023
		Contract Term: *(From Effective Date)*	<u>09/08/2023 - 09/07/2024</u>
		Annual License Fee:	$6,500 / year
Panorama Survey Platform ● Student Surveys ● Teacher & Staff Surveys ● Family Surveys		***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.