West Virginia Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

wv OASIS

Jump to: FORMS | Go | Home | Personalize | Accessibility | App Help | About

Welcome, Lu Anne Cottrill | Procurement | Budgeting | Accounts Receivable | Accounts Payable

Solicitation Response(SR) | Dept: 0225 | ID: ESR08192000000001083 | Ver.: 1 | Function: New | Phase: Final | Modified by batch , 08/19/2020

Header 🔗 14

List View

General Information | Contact | Default Values | Discount | Document Information

Procurement Folder: 715719	**SO Doc Code:** CRFQ
Procurement Type: Central Contract - Fixed Amt	**SO Dept:** 0225
Vendor ID: 000000209693	**SO Doc ID:** PEI2100000001
Legal Name: INTELLIPOINT TECHNOLOGIES LLC	**Published Date:** 8/18/20
Alias/DBA:	**Close Date:** 8/19/20
Total Bid: $0.00	**Close Time:** 13:30
Response Date: 08/19/2020	**Status:** Closed
Response Time: 13:16	**Solicitation Description:** Addendum No. 4 MICROSOFT DYNAMICS GP & RELATED
	Total of Header Attachments: 14
	Total of All Attachments: 14

Proc Folder : 715719

Solicitation Description : Addendum No. 4 MICROSOFT DYNAMICS GP & RELATED LICENSES

Proc Type : Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-08-19 13:30:00	SR 0225 ESR08192000000001083	1

VENDOR
000000209693
INTELLIPOINT TECHNOLOGIES LLC

Solicitation Number: CRFQ   0225   PEI2100000001

Total Bid : $0.00   **Response Date:**   2020-08-19   **Response Time:**   13:16:06

Comments:

FOR INFORMATION CONTACT THE BUYER

Melissa Pettrey

(304) 558-0094
melissa.k.pettrey@wv.gov

Signature on File   **FEIN #**   **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	MICROSOFT GP Related Software	0.00000	EA	$1,043,421.400000	$0.00

Comm Code	Manufacturer	Specification	Model #
43231512			

Extended Description : ENTER TOTAL BID AMOUNT FROM EXHIBIT A PRICING SHEET HERE

Comments: Spreadsheet has incorrect formulas. In addition to Appendix A we are submitting a corrected spreadsheet.

EXHIBIT A - PRICING PAGE - Modified for Addendum 4

The costs listed are considered firm during the awarded contract. Ancillary expenses (travel, meals, lodging, etc) are to be included in proposed rates and will not be paid directly. Additional copies of this page should be used in the event that the Vendor intends to include price adjustments over the initial Contract term (5 years).

Spec Item Ref	Item	Est. Qty	Year One through Five (Cost per Qty)	Extended Cost Year 1-5	Year Six (optional renewal)	Extended Cost Year 6	Year Seven (optional renewal)	Extended Cost year 7	Year Eight (optional renewal)	Extended Cost Year 8	Extended Cost Years 1 - 8
4.1	**License Renewal Fees**										
4.1.1	Dynamics GP	16	$ 761.30	$ 60,904.00	$ 761.30	$ 12,180.80	$ 761.30	$ 12,180.80	$ 761.30	$12,180.80	$ 97,446.40
4.1.2	eOne	1	$ 770.00	$ 3,850.00	$ 770.00	$ 770.00	$ 770.00	$ 770.00	$ 770.00	$ 770.00	$ 6,160.00
4.1.3	Professional Advantage	1	$ 1,280.00	$ 6,400.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 10,240.00
4.1.4	Merit Solutions - 1 License	1	$ 1,200.00	$ 6,000.00	$ 1,200.00	$ (1,200.00)	$ 1,200.00	$ 1,200.00	$ 1,200.00	$ 1,200.00	$ 7,200.00
4.1.5	**Software Maintenance and Support Services***										
4.1.5.1	Upgrade services (per upgrade)	1	$ 21,375.00	$ 106,875.00	$21,375.00	$ (21,375.00)	$ 21,375.00	$ 21,375.00	$ 21,375.00	$21,375.00	$ 128,250.00
4.1.5.2	Patch installation (per installation)	5	$ 2,137.50	$ 53,437.50	$ 2,137.50	$ (10,687.50)	$ 2,137.50	$ 10,687.50	$ 2,137.50	$10,687.50	$ 64,125.00
4.1.5.3	Functional requirement development cost (per hr)	250	$ 200.00	$ 250,000.00	$ -	$ -	$ -	$ -	$ -	$ -	$ 250,000.00
4.1.5.4	Performance issue and support ticket consulting services by criticality (per hour)										
	Low	80	$ 200.00	$ 80,000.00	$ 200.00	$ (16,000.00)	$ 200.00	$ 16,000.00	$ 200.00	$16,000.00	$ 96,000.00
	Moderate	48	$ 200.00	$ 48,000.00	$ 200.00	$ (9,600.00)	$ 200.00	$ 9,600.00	$ 200.00	$ 9,600.00	$ 57,600.00
	High	40	$ 200.00	$ 40,000.00	$ 200.00	$ (8,000.00)	$ 200.00	$ 8,000.00	$ 200.00	$ 8,000.00	$ 48,000.00
	Critical	32	$ 200.00	$ 32,000.00	$ 200.00	$ (6,400.00)	$ 200.00	$ 6,400.00	$ 200.00	$ 6,400.00	$ 38,400.00
4.1.5.5	User training (per hour)	200	$ 200.00	$ 200,000.00	$ 200.00	$ (40,000.00)	$ 200.00	$ 40,000.00	$ 200.00	$40,000.00	$ 240,000.00
									TOTAL BID AMOUNT		$ 1,043,421.40

*Payable as service rendered

Contract will be evaluated on TOTAL BID AMOUNT but **only awarded on** years 1-5.

Renewal options for years 6, 7, and 8 will be initiated by the Agency, agreed to by the Vendor and Processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

The costs listed are considered firm during the awarded contract. Ancillary expenses (travel, meals, lodging, etc) are to be included in proposed rates and will not be paid directly. Additional copies of this page should be used in the event that the Vendor intends to include price adjustments over the initial Contract term (5 years).

Spec Item Ref	Item	Est. Qty	Year One through Five (Cost per Qty)	Extended Cost Year 1-5	Year Six (optional renewal)	Extended Cost Year 6	Year Seven (optional renewal)	Extended Cost year 7	Year Eight (optional renewal)	Extended Cost Year 8	Extended Cost Years 1 - 8
4.1	**License Renewal Fees**										
4.1.1	Dynamics GP	1	$ 12,180.80	$ 60,904.00	$ 12,180.80	$ 12,180.80	$ 12,180.80	$ 12,180.80	$ 12,180.80	$ 12,180.80	$ 97,446.40
4.1.2	eOne	1	$ 770.00	$ 3,850.00	$ 770.00	$ 770.00	$ 770.00	$ 770.00	$ 770.00	$ 770.00	$ 6,160.00
4.1.3	Professional Advantage	1	$ 1,280.00	$ 6,400.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 1,280.00	$ 10,240.00
4.1.4	Merit Solutions - 1 License	1	$ 1,200.00	$ 6,000.00	$ 1,200.00	$ 1,200.00	$ 1,200.00	$ 1,200.00	$ 1,200.00	$ 1,200.00	$ 9,600.00
4.1.5	**Software Maintenance and Support Services***										
4.1.5.1	Upgrade services (per upgrade)	1	$ 21,375.00	$ 106,875.00	$ 21,375.00	$ 21,375.00	$ 21,375.00	$ 21,375.00	$ 21,375.00	$ 21,375.00	$ 171,000.00
4.1.5.2	Patch installation (per installation)	5	$ 2,137.50	$ 53,437.50	$ 2,137.50	$ 10,687.50	$ 2,137.50	$ 10,687.50	$ 2,137.50	$ 10,687.50	$ 85,500.00
4.1.5.3	Functional requirement development cost (per hr)	250	$ 200.00	$ 250,000.00	$ -	$ -	$ -	$ -	$ -	$ -	$ 250,000.00
4.1.5.4	Performance issue and support ticket consulting services by criticality (per hour)										
	Low	80	$ 200.00	$ 80,000.00	$ 200.00	$ 16,000.00	$ 200.00	$ 16,000.00	$ 200.00	$ 16,000.00	$ 128,000.00
	Moderate	48	$ 200.00	$ 48,000.00	$ 200.00	$ 9,600.00	$ 200.00	$ 9,600.00	$ 200.00	$ 9,600.00	$ 76,800.00
	High	40	$ 200.00	$ 40,000.00	$ 200.00	$ 8,000.00	$ 200.00	$ 8,000.00	$ 200.00	$ 8,000.00	$ 64,000.00
	Critical	32	$ 200.00	$ 32,000.00	$ 200.00	$ 6,400.00	$ 200.00	$ 6,400.00	$ 200.00	$ 6,400.00	$ 51,200.00
4.1.5.5	User training (per hour)	200	$ 200.00	$ 200,000.00	$ 200.00	$ 40,000.00	$ 200.00	$ 40,000.00	$ 200.00	$ 40,000.00	$ 320,000.00
									TOTAL BID AMOUNT		$ 1,269,946.40

*Cell C6 should only be 1. Corrected cells G9, G11-13, G15-19. Formula had negative in it. Corrected to positive.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: PEI2100000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

☑ Addendum No. 1   ☐ Addendum No. 6
☑ Addendum No. 2   ☐ Addendum No. 7
☑ Addendum No. 3   ☐ Addendum No. 8
☑ Addendum No. 4   ☐ Addendum No. 9
☐ Addendum No. 5   ☐ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

_____
Company

_____
Authorized Signature

_____
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 01/09/2020

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _INTELLIPOINT TECHNOLOGIES LLC_

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☐
   No ☐

2. If yes to #1, does the restricted information include personal data?
   Yes ☐
   No ☐

3. If yes to #1, does the restricted information include non-public data?
   Yes ☐
   No ☐

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☐

5. Provide name and email address for the Department privacy officer:

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: _DENNIS A. BARRY_

   Email address: _dennis.barry@intellipoint.net_

   Phone Number: _304 733-3687_

Attachment D
DATA MANAGEMENT ADDENDUM & APPENDIX

Data Exchange – Data Management Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

<u>Public Jurisdiction</u> means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

<u>Public Jurisdiction Data</u> means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

<u>Public Jurisdiction Identified Contact</u> means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

<u>Restricted data</u> means personal data and non-public data.

<u>Security Incident</u> means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

<u>Service Provider</u> means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

<u>Software-as-a-Service (SaaS)</u> means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:
   a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

   a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

   b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

   c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

   a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:
  a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
  b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
  c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
    - 10 days after the effective date of termination, if the termination is in accordance with the contract period
    - 30 days after the effective date of termination, if the termination is for convenience
    - 60 days after the effective date of termination, if the termination is for cause

  After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.
  d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
  e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:
   a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

7

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

8

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:
   a. Access and use the service for its business purposes;
   b. For SaaS, use underlying software as embodied or used in the service; and
   c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency:_____

Signature:_____

Title:_____

Date:_____

Name of Vendor: INTELLIPOINT TECH NOLOGIES

Signature: _____

Title: CEO

Date: 8/13/2000

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate"), and is effective as of the date of execution of the Addendum.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to disclose to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

   a. **Agency Procurement Officer** shall mean the appropriate Agency individual listed at: http://www.state.wv.us/admin/purchase/vrc/agencyli.html.

   b. **Agent** shall mean those person(s) who are agent(s) of the Business Associate, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c).

   c. **Breach** shall mean the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.

   d. **Business Associate** shall have the meaning given to such term in 45 CFR § 160.103.

   e. **HITECH Act** shall mean the Health Information Technology for Economic and Clinical Health Act. Public Law No. 111-05. 111th Congress (2009).

f.   **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164.

g.   **Protected Health Information or PHI** shall have the meaning given to such term in 45 CFR § 160.103, limited to the information created or received by Associate from or on behalf of Agency.

h.   **Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.

i.   **Security Rule** means the Security Standards for the Protection of Electronic Protected Health Information found at 45 CFR Parts 160 and 164.

j.   **Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

2. **Permitted Uses and Disclosures.**

a.   **PHI Described.** This means PHI created, received, maintained or transmitted on behalf of the Agency by the Associate. This PHI is governed by this Addendum and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the original Agreement, and is described in Appendix A.

b.   **Purposes.** Except as otherwise limited in this Addendum, Associate may use or disclose the PHI on behalf of, or to provide services to, Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the original Agreement, or as required by law, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Agency or Associate, or violate the minimum necessary and related Privacy and Security policies and procedures of the Agency. The Associate is directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Agency.

c.   **Further Uses and Disclosures.** Except as otherwise limited in this Addendum, the Associate may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that (i) the disclosure is required by law, or (ii) the Associate has obtained from the third party reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by the Associate; and, (iii) an agreement to notify the Associate and Agency of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached. To the extent practical, the information should be in a limited data set or the minimum necessary information pursuant to 45 CFR § 164.502, or take other measures as necessary to satisfy the Agency's obligations under 45 CFR § 164.502.

3. **Obligations of Associate.**

   a. **Stated Purposes Only.** The PHI may not be used by the Associate for any purpose other than as stated in this Addendum or as required or permitted by law.

   b. **Limited Disclosure.** The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Agency gives written approval and the individual provides a valid authorization. Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Associate will report to Agency any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.

   c. **Safeguards.** The Associate will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to:

      i. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;

      ii. Appropriate notification and training of its workforce and agents in order to protect the PHI from unauthorized use and disclosure;

      iii. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations, in compliance with the Security Rule;

      iv. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

   d. **Compliance With Law.** The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules.

   e. **Mitigation.** Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum, and report its mitigation activity back to the Agency.

f. **Support of Individual Rights.**

    i.   **Access to PHI.** Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying, and in electronic format, if requested, within ten (10) days of a request by Agency to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.

    ii.   **Amendment of PHI.** Within ten (10) days of receipt of a request from Agency for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Agency for amendment and incorporate any such amendment to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526.

    iii.   **Accounting Rights.** Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Agency the documentation required to provide an accounting of disclosures to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR §164.528 and consistent with Section 13405 of the HITECH Act. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:

- the date of disclosure;
- the name of the entity or person who received the PHI, and if known, the address of the entity or person;
- a brief description of the PHI disclosed; and
- a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

    iv.   **Request for Restriction.** Under the direction of the Agency, abide by any individual's request to restrict the disclosure of PHI, consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522, when the Agency determines to do so (except as required by law) and if the disclosure is to a health plan for payment or health care operations and it pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."

    v.   **Immediate Discontinuance of Use or Disclosure.** The Associate will immediately discontinue use or disclosure of Agency PHI pertaining to any individual when so requested by Agency. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

g. **Retention of PHI.** Notwithstanding section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Addendum for a period of six (6) years after termination of the Agreement, or longer if required under state law.

h. **Agent's, Subcontractor's Compliance.** The Associate shall notify the Agency of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract and shall be delivered to the Agency Procurement Officer. The Associate will ensure that any of its subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Agency, agree to the restrictions and conditions which apply to the Associate hereunder. The Agency may request copies of downstream subcontracts and agreements to determine whether all restrictions, terms and conditions have been flowed down. Failure to ensure that downstream contracts, subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement.

j. **Federal and Agency Access.** The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by the Associate on behalf of the Agency available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504. The Associate shall also make these records available to Agency, or Agency's contractor, for periodic audit of Associate's compliance with the Privacy and Security Rules. Upon Agency's request, the Associate shall provide proof of compliance with HIPAA and HITECH data privacy/protection guidelines, certification of a secure network and other assurance relative to compliance with the Privacy and Security Rules. This section shall also apply to Associate's subcontractors, if any.

k. **Security.** The Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII is required, to the extent practicable. If Associate chooses not to adopt such methodologies as defined in 74 FR 19006 to secure the PHI governed by this Addendum, it must submit such written rationale, including its Security Risk Analysis, to the Agency Procurement Officer for review prior to the execution of the Addendum. This review may take up to ten (10) days.

l. **Notification of Breach.** During the term of this Addendum, the Associate shall notify the Agency and, unless otherwise directed by the Agency in writing, the WV Office of Technology immediately by e-mail or web form upon the discovery of any Breach of unsecured PHI; or within 24 hours by e-mail or web form of any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Agency Procurement Officer at www.state.wv.us/admin/purchase/vrc/agencyli.htm and,

5

unless otherwise directed by the Agency in writing, the Office of Technology at incident@wv.gov or https://apps.wv.gov/ot/ir/Default.aspx.

The Associate shall immediately investigate such Security Incident, Breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, the Associate shall notify the Agency Procurement Officer, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.

If the Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Agency Procurement Officer. Failure to include such requirement in any subcontract or agreement may result in the Agency's termination of the Agreement.

m. **Assistance in Litigation or Administrative Proceedings.** The Associate shall make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

4. Addendum Administration.

a. **Term.** This Addendum shall terminate on termination of the underlying Agreement or on the date the Agency terminates for cause as authorized in paragraph (c) of this Section, whichever is sooner.

b. **Duties at Termination.** Upon any termination of the underlying Agreement, the Associate shall return or destroy, at the Agency's option, all PHI received from, or created or received by the Associate on behalf of the Agency that the Associate still maintains in any form   and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Addendum to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents

6

and subcontractors to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

    c. **Termination for Cause.** Associate authorizes termination of this Agreement by Agency, if Agency determines Associate has violated a material term of the Agreement. Agency may, at its sole discretion, allow Associate a reasonable period of time to cure the material breach before termination.

    d. **Judicial or Administrative Proceedings.** The Agency may terminate this Agreement if the Associate is found guilty of a criminal violation of HIPAA. The Agency may terminate this Agreement if a finding or stipulation that the Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the Associate is a party or has been joined. Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.

    e. **Survival.** The respective rights and obligations of Associate under this Addendum shall survive the termination of the underlying Agreement.

5. **General Provisions/Ownership of PHI.**

    a. **Retention of Ownership.** Ownership of the PHI resides with the Agency and is to be returned on demand or destroyed at the Agency's option, at any time, and subject to the restrictions found within section 4.b. above.

    b. **Secondary PHI.** Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Agency.

    c. **Electronic Transmission.** Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Agency.

    d. **No Sales.** Reports or data containing the PHI may not be sold without Agency's or the affected individual's written consent.

    e. **No Third-Party Beneficiaries.** Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Agency, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

    f. **Interpretation.** The provisions of this Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.

    g. **Amendment.** The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.

    h. **Additional Terms and Conditions.** Additional discretionary terms may be included in the release order or change order process.
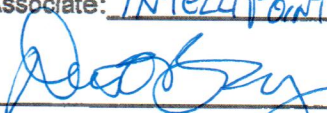
AGREED:

Name of Agency:_____

Signature:_____

Title:_____

Date:_____

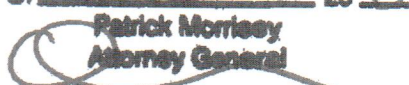Name of Associate: _INTELLIPOINT TECHNOLOGIES_

Signature: _[signature]_

Title: _CEO_

Date: _8/13/2020_

Form - WVBAA-012004
Amended 06.26.2013

APPROVED AS TO FORM THIS 26th
DAY OF _Jan_ 20 _11_
Patrick Morrisey
Attorney General
BY _____

Appendix A

Name of Associate: _INTELLIPOINT TECHNOLOGIES_ , hereafter
referred to as the GP Support and Maintenance Vendor

Name of Agency(ies): The West Virginia Public Employees Insurance Agency (PEIA

Describe the PHI. If not applicable please indicate the same.

Per 45 CFR, Part 160.103

Health information means any information, whether oral or recorded in any form or medium,
that:

(1) Is created or received by a health care provider, health plan, public health authority,
employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an
individual; the provision of health care to an individual; or the past, present, or future
payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information,
including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care
clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an
individual; the provision of health care to an individual; or the past, present, or future
payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information
can be used to identify the individual.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

The information provided to, transmitted by, and/or created by the Associate and/or stored
and/or maintained by the Associate in electronic form(s) on platform(s) owned, managed and/or

administered by the Associate, pursuant to the Agreement will include the minimum necessary to perform the services thereunder and will specifically include, but may not be limited to:

a) The Associate, as the defined "Business Partner" will provide licensing and accompanying administrative, technical, and/or procedural support to the Covered Entity for the Covered Entity's "Great Plains" application(s) and/or in related applications used to support the "Great Plains" application(s).

b) PEIA member individually identifiable health information or protected health information, including but not necessarily limited to, name(s), names of dependent(s), specific identifying information, e.g. address(es), date(s) of birth, social security number(s), policy number(s), etc. that may be viewable in the "Great Plains" application(s) and/or in related applications used to support the "Great Plains" application(s).

c) PEIA member individually identifiable health information or protected health information necessary to allow the Covered Entity to perform their statutory business function(s) in accordance with State and/or Federal law(s) that may be viewable in the "Great Plains" application(s) and/or in related applications used to support the "Great Plains" application(s).

d) PEIA member individually identifiable health information protected health information used in relation to interfaces with public websites and/or portals or internal websites and/or portals that may be viewable in the "Great Plains" application(s) and/or in related applications used to support the "Great Plains" application(s).

e) PEIA member protected health information needed by and/or for other identified Business Associates in the provision of their services to the Covered Entity that involves access to protected health information.

f) PEIA member protected health information posted to file transfer protocol (FTP) site(s) for delivery, transmission, or receipt by other Business Associate(s) of the Covered Entity(ies) that may be viewable in the "Great Plains" application(s) and/or in related applications used to support the "Great Plains" application(s).

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 715719

Doc Description: Addendum No. 1 MICROSOFT DYNAMICS GP & RELATED LICENSES

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2020-08-03	2020-08-13 13:30:00	CRFQ 0225 PEI2100000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON   WV   25305
US

VENDOR

Vendor Name, Address and Telephone Number:

FOR INFORMATION CONTACT THE BUYER

Melissa Pettrey
(304) 558-0094
melissa.k.pettrey@wv.gov

Signature X _____   FEIN #   550759379   DATE 8/13/2020

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

Addendum

Addendum No. 1 is issued to publish and distribute the attached information to the vendor community.
****

Request for Quotation

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Public Employees Agency (PEIA) to establish a contract for software maintenance and support of the following licenses, which PEIA currently own and use:
Microsoft GP 2016 ; eOne; Professional Advantage; and Merit Solutions, per the Specifications, Bid requirements and Terms and Conditions as attached hereto.

INVOICE TO	SHIP TO
PUBLIC EMPLOYEES INSURANCE STE 2 601 57TH ST SE CHARLESTON WV 25304 US	PUBLIC EMPLOYEES INSURANCE STE 2 601 57TH ST, SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	MICROSOFT GP Related Software	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231512			

Extended Description :

ENTER TOTAL BID AMOUNT FROM EXHIBIT A PRICING SHEET HERE

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia
Request for Quotation
21 — Info Technology**

Proc Folder: 715719

Doc Description: Addendum No. 2 MICROSOFT DYNAMICS GP & RELATED LICENSES.

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2020-08-12	2020-08-17 13:30:00	CRFQ 0225 PEI2100000001	3

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON   WV   25305
US

VENDOR

Vendor Name, Address and Telephone Number:

FOR INFORMATION CONTACT THE BUYER

Melissa Pettrey
(304) 558-0094
melissa.k.pettrey@wv.gov

Signature X _(signature)_   FEIN # 55-0759379   DATE 8/13/2020

All offers subject to all terms and conditions contained in this solicitation

Addendum

Addendum No. 2 is issued to publish and distribute the attached information to the vendor community.
****

Request for Quotation

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Public Employees Agency (PEIA) to establish a contract for software maintenance and support of the following licenses, which PEIA currently own and use:
Microsoft GP 2016 ; eOne; Professional Advantage; and Merit Solutions, per the Specifications, Bid requirements and Terms and Conditions as attached hereto.

INVOICE TO	SHIP TO
PUBLIC EMPLOYEES INSURANCE STE 2 601 57TH ST SE CHARLESTON WV 25304 US	PUBLIC EMPLOYEES INSURANCE STE 2 601 57TH ST, SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	MICROSOFT GP Related Software	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231512			

Extended Description :

ENTER TOTAL BID AMOUNT FROM EXHIBIT A PRICING SHEET HERE

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 715719

Doc Description: Addendum No. 3 MICROSOFT DYNAMICS GP & RELATED LICENSES

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No		Version
2020-08-13	2020-08-19 13:30:00	CRFQ	0225 PEI2100000001	4

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON   WV   25305

US

VENDOR

Vendor Name, Address and Telephone Number:

FOR INFORMATION CONTACT THE BUYER

Melissa Pettrey
(304) 558-0094
melissa.k.pettrey@wv.gov

Signature X _(signature)_   **FEIN #** 55 0759379   **DATE** 8/13/2020

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

Addendum

Addendum No. 3 is issued to publish and distribute the attached information to the vendor community.
****

Request for Quotation

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Public Employees Agency (PEIA) to establish a contract for software maintenance and support of the following licenses, which PEIA currently own and use:
Microsoft GP 2016 ; eOne; Professional Advantage; and Merit Solutions, per the Specifications, Bid requirements and Terms and Conditions as attached hereto.

INVOICE TO		SHIP TO	
PUBLIC EMPLOYEES INSURANCE STE 2		PUBLIC EMPLOYEES INSURANCE STE 2	
601 57TH ST SE		601 57TH ST, SE	
CHARLESTON	WV 25304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	MICROSOFT GP Related Software	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231512			

Extended Description :
ENTER TOTAL BID AMOUNT FROM EXHIBIT A PRICING SHEET HERE

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — **Info Technology**

Proc Folder: 715719

Doc Description: Addendum No. 4 MICROSOFT DYNAMICS GP & RELATED LICENSES

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2020-08-18	2020-08-19 13:30:00	CRFQ 0225 PEI2100000001	5

BID RECEIVING LOCATION
BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON   WV   25305
US

VENDOR
Vendor Name, Address and Telephone Number:

FOR INFORMATION CONTACT THE BUYER
Melissa Pettrey
(304) 558-0094
melissa.k.pettrey@wv.gov

Signature X _____ FEIN # 55-0759379 DATE 8/19/2020

All offers subject to all terms and conditions contained in this solicitation

FORM ID : WV-PRC-CRFQ-001

Addendum

Addendum No. 4 is issued to correct cell G7 and E13 on the Exhibit A Pricing Page, and to clarify that Column D is for an extended cost for the first five years of the contract. Vendors should enter the cost per quantity in Column D, the Extended Cost in Column E is determined by the Cost Per Quantity multiplied by Estimated Quantity, multiplied by five (5) for a total extended cost for 5 years in Column E.

For Vendors that have already submitted a bid and used the original version of the spreadsheet, unit cost prevails and the extended cost will be corrected for evaluation purposes.

No other changes

INVOICE TO	SHIP TO
PUBLIC EMPLOYEES INSURANCE STE 2 601 57TH ST SE CHARLESTON WV 25304 US	PUBLIC EMPLOYEES INSURANCE STE 2 601 57TH ST, SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	MICROSOFT GP Related Software	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231512			

Extended Description :
ENTER TOTAL BID AMOUNT FROM EXHIBIT A PRICING SHEET HERE

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 715719

Doc Description: MICROSOFT DYNAMICS GP & RELATED LICENSES

Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No		Version
2020-07-23	2020-08-06 13:30:00	CRFQ	0225 PEI2100000001	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON   WV   25305
US

VENDOR

Vendor Name, Address and Telephone Number:

FOR INFORMATION CONTACT THE BUYER

Melissa Pettrey
(304) 558-0094
melissa.k.pettrey@wv.gov

Signature X _(signature)_   FEIN # 55-0739379   DATE 8/13/2020

All offers subject to all terms and conditions contained in this solicitation

Request for Quotation

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Public Employees Agency (PEIA) to establish a contract for software maintenance and support of the following licenses, which PEIA currently own and use:
Microsoft GP 2016 ; eOne; Professional Advantage; and Merit Solutions, per the Specifications, Bid requirements and Terms and Conditions as attached hereto.

INVOICE TO		SHIP TO	
PUBLIC EMPLOYEES INSURANCE STE 2		PUBLIC EMPLOYEES INSURANCE STE 2	
601 57TH ST SE		601 57TH ST, SE	
CHARLESTON	WV 25304	CHARLESTON	WV 25304
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	MICROSOFT GP Related Software	0.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231512			

Extended Description :
ENTER TOTAL BID AMOUNT FROM EXHIBIT A PRICING SHEET HERE

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Attachment F
Vendor Personnel Resumes

Vendor Personnel Resume

Name	Thomas Gibas
Title	Senior Applications Consultant
Relevant Experience	Microsoft Dynamics GP Version 7.5 - Current (Installs, Migration, Upgrades, Patching, & Troubleshooting) Third Party Integrations into GP (Patching, Upgrades, and Installs) Reporting Software with GP (MR, FRx, SQL Reporting Services) SQL 2000 - Current (Installs, Patching, Upgrade, Migrations & Troubleshooting)
Relevant Certifications	MS Dynamics GP Install and Config; Scribe
Education	4 Years Marshall University
	13 Years Experience working with Dynamics GP & SQL
	30 Years working with Networking and Windows

Vendor Personnel Resume

Name	Rebecka Jarrell
Title	Applications Technician
Relevant Experience	Microsoft Dynamics GP Version 2010 - Current (Installs, Upgrades, Patching, & Troubleshooting) Microsoft Dynamics GP Version 2010 - Current (Support, Data Migration, and Setup for Financial, AP, AR, POP, SOP, Payroll & HR, Inventory) Third Party Integration to GP (Patching, Upgrades, and Installs as well as setup and troubleshooting product) Reporting Software (MR, FRx, SQL Reporting Services, and Refreshable Excel Docs - Setup, Install, Updates, and report creation)
Relevant Certifications	MS Dynamics GP Install & Config; MS Dynamics GP Financials; Accounting Coach
Education	4 Years Masrhall University
	5 Years Experience Working with Dynamics GP, SQL
	5 Years Experiences with Accounting Softwares and Setup

Vendor Personnel Resume

Name	
Title	
Relevant Experience	
Relevant Certifications	
Education	

Vendor Personnel Resume

Name	
Title	
Relevant Experience	
Relevant Certifications	
Education	

REQUEST FOR PROPOSAL – [RFP DESCRIPTION]

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code §61-5-3*) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Intellipoint Technologies, LLC

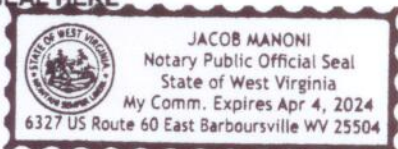Authorized Signature: Rebecka Overell   Date: 08/19/20

State of West Virginia

County of Cabell , to-wit:

Taken, subscribed, and sworn to before me this 19th day of August , 2020.

My Commission expires April 4th , 2020.

AFFIX SEAL HERE   NOTARY PUBLIC _____

Purchasing Affidavit (Revised 01/19/2018)

Attachment E

Vendor Experience Reference Information

Reference #1 (Required)

Contact Person	Tim Burgess
Position	CFO
Address	1 Zims Ln
City, State, Zip	Prichard, WV 25555
Telephone Number	304-486-5651
E-mail Address	timburgess@zimsbagging.com
Project Description	Dynamics GP, SQL, and Server Upgrade
Project Dates	Dynamics GP Upgrade - Annual; Dec 2019 Last Performed
Personnel Assigned	Tom Gibas

Reference #2 (Required)

Contact Person	Justin Evans
Position	Accounting Manager
Address	500 Leon Sullivan Way
City, State, Zip	Charleston, WV 25301
Telephone Number	304-556-1190
E-mail Address	jevans@utalent.com
Project Description	Bullhorn Payroll Integration into GP & GP Payroll Setup Yearly GP Year end Update every December 3rd Party Product Setup for Payroll Security 05/19-06/19 New GP Company Setup - 08/19-09/19
Project Dates	November 2018- May 2019 Payroll Integration and Setup
Personnel Assigned	Rebecka Jarrell

Vendor Experience Reference Information

Reference #3 (Required)

Contact Person	Pamela Fauver
Position	Accounting Manager
Address	166 Jack Burlingame Drive
City, State, Zip	Millwood, WV 25262
Telephone Number	1-800-788-3867
E-mail Address	pam@lloydselectronics.com
Project Description	Sharepoint Site Setup - 07/20-08/20 GP Year End Update - Annualy, Last on 12/19 Setup Emailing Invoices to Customers in GP - 06/19 - 9/19
Project Dates	See Above
Personnel Assigned	Rebecka Jarrell

Reference #4 (Optional)

Contact Person	
Position	
Address	
City, State, Zip	
Telephone Number	
E-mail Address	
Project Description	
Project Dates	
Personnel Assigned	