Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	**State of West Virginia** # Master Agreement **Order Date:** 12-18-2024	CORRECT ORDER NUMBER MUST APPEAR ON ALL PACKAGES, INVOICES, AND SHIPPING PAPERS. QUESTIONS CONCERNING THIS ORDER SHOULD BE DIRECTED TO THE DEPARTMENT CONTACT.

Order Number:	CMA 0803 0081 DOT2300000025 4	**Procurement Folder:**	1119410
Document Name:	dTIMS Software Subscription & Support	**Reason for Modification:**	
Document Description:	CO 3 - dTIMS Software (81250043)	Change Order 3 To Add Executed SaaS Addendum	
Procurement Type:	Central Sole Source		
Buyer Name:			
Telephone:			
Email:			
Shipping Method:	Best Way	**Effective Start Date:**	2022-12-01
Free on Board:	FOB Dest, Freight Prepaid	**Effective End Date:**	2025-11-30

VENDOR	DEPARTMENT CONTACT
Vendor Customer Code: 000000233045 DEIGHTON ASSOCIATES LTD 1555 WENTWORTH ST UNIT 200 WHITBY ON L1N 9T6 CA **Vendor Contact Phone:** 9056656605 **Extension:** 132	**Requestor Name:** Sidney Oliver **Requestor Phone:** 304-414-7119 **Requestor Email:** jr.oliver@wv.gov

Discount Details:

	Discount Allowed	Discount Percentage	Discount Days
#1	No	0.0000	0
#2	No		
#3	No		
#4	No		

2025
FILE LOCATION _____

INVOICE TO	SHIP TO
INFORMATION TECHNOLOGY DIVISION DEPT. OF TRANSPORTATION 1900 KANAWHA BLVD E, BLD. 5 RM-720 CHARLESTON WV 25305 US	INFORMATION TECHNOLOGY DIVISION DEPT. OF TRANSPORTATION 1900 KANAWHA BLVD E, BLD. 5 RM-720 CHARLESTON WV 25305 US

CR 12-19-24

Total Order Amount:	Open End

Purchasing Division's File Copy

SE 12/18/24

PURCHASING DIVISION AUTHORIZATION	ATTORNEY GENERAL APPROVAL AS TO FORM	ENCUMBRANCE CERTIFICATION
DATE: 12-19-24 ELECTRONIC SIGNATURE ON FILE	DATE: John S. Gross ELECTRONIC SIGNATURE ON FILE	DATE: 12-20-24 ELECTRONIC SIGNATURE ON FILE

12/20/2024

Extended Description:
Change Order

Change Order No. 3 is issued to add the Executed SaaS Addendum as required by the Office of Technology.

No other changes.

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
1	81112200				0.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: dTIMS Subscription and Support

Extended Description:
dTIMS Subscription and Support

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
2	81112200				0.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: dTIMS Subscription and Support Y2

Extended Description:
dTIMS Subscription and Support

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
3	81112200				0.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: dTIMS Subscription and Support Y3

Extended Description:
dTIMS Subscription and Support

WEST VIRGINIA DEPARTMENT OF TRANSPORTATION
Division of Highways
1900 Kanawha Boulevard East • Building Five • Room 110
Charleston, West Virginia 25305-0430 • (304) 558-3505

Alanna J. Keller, P.E.
Deputy Secretary of Transportation
Deputy Commissioner of Highways

Jimmy Wriston, P. E.
Secretary of Transportation
Commissioner of Highways

This amendment, effective November 15, 2024, is between the WV Department of Transportation, Division of Highways ("DOH") and Deighton Associates, Ltd. ("Deighton")(collectively WVDOH and Deighton are "the Parties"), amends the dTIMS Software Subscription & Support Master Agreement between the Parties having an order date of October 15, 2024 ("Master Agreement"), and all extensions thereto.

The Software as a Service ("SaaS") Addendum and its Appendix A (both attached and initialed), incorporate the full terms and conditions of the Master Agreement.

The SaaS Addendum authorizes Deighton to retain a subcontractor for certain on-premise services related to accessing certain dTIMS software licensed by Deighton to WVDOH.

WVDOT

Hussein S ELKhansa
Signature

CTO
Title

Deighton

DocuSigned by:
Robert Piane P.Eng.
FA3FAD020E0A4D8...
Signature

President / Director
Title

Software as a Service 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

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.

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

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

Restricted data means personal data and non-public data. Security Incident 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.

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

Software-as-a-Service (SaaS) 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:

- 30 days after the effective date of termination, if the termination is in accordance with the contract period;
- 60 days after the effective date of termination, if the termination is for convenience;
- 90 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 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 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, during the term of the subscription, 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: WVDOT Hussein S ELKHANSA

Signature: Hussein S ELKhansa

Title: CTO

Date: 11/25/2024

Name of Vendor: Deighton Associates Ltd

Signature: DocuSigned by: Robert Piane P.Eng. FA3FAD020E0A4DB...

Title: President / Director

Date: 11/18/2024 | 10:07 AM EST

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: Deighton Associates Ltd.

Name of Agency: West Virginia Department of Transportation

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes [X]
   No [ ]

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

3. If yes to #1, does the restricted information include non-public data?
   Yes [X]
   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 [X]

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

   Name: Jonathan Schaffer

   Email address: jonathan.w.schaffer@wv.gov

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: Brock Deighton

   Email address: Brock@Deighton.com

   Phone Number: (905) 435 5572

You are viewing this page over a secure connection. Click here for more information.

West Virginia Secretary of State — Online Data Services

Business and Licensing

Online Data Services Help

Business Organization Detail

NOTICE: The West Virginia Secretary of State's Office makes every reasonable effort to ensure the accuracy of information. However, we make no representation or warranty as to the correctness or completeness of the information. If information is missing from this page, it is not in the The West Virginia Secretary of State's database.

DEIGHTON ASSOCIATES LTD.

Organization Information

Org Type	Effective Date	Established Date	Filing Date	Charter	Class	Sec Type	Termination Date	Termination Reason
C | Corporation	5/13/1992		5/13/1992	Foreign	Profit			

Organization Information

Business Purpose	*5182 - Information - Data* Processing, Hosting, and Related Services - Data Processing, Hosting and Related Services	**Capital Stock**	0.0000
Charter County	Foreign Country	**Control Number**	0
Charter State	ONT	**Excess Acres**	0
At Will Term		**Member Managed**	
At Will Term Years		***Par Value***	*0.000000*
Authorized Shares	0	**Young Entrepreneur**	Not Specified

Addresses

Type	Address
Local Office Address	1555 WENTWORTH ST UNIT 200 WHITBY, ON, L1N 9T6
Mailing Address	1555 WENTWORTH ST UNIT 200 WHITBY, ON, L1N 9T6 CAN
Notice of Process Address	*CORPORATION SERVICE COMPANY* 209 WEST WASHINGTON STREET CHARLESTON, WV, 25302
Principal Office Address	1555 WENTWORTH ST UNIT 200 WHITBY, ON, L1N 9T6 CAN
Type	**Address**

Officers

Type	Name/Address
Director	ROB PIANE 1555 WENTWORTH ST UNIT 200 WHITBY, ON, L1N 9T6
President	VICKI DEIGHTON 1555 WENTWORTH ST UNIT 200 WHITBY, ON, L1N 9T6
Type	**Name/Address**

Annual Reports

Filed For
2024
2023
2022
2021
2020
2019

2018
2017x
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007
2004
2003
2002
2001
2000
1999
Date filed

For more information, please contact the Secretary of State's Office at 304-558-8000.

Wednesday, December 18, 2024 — 12:18 PM

SAM.GOV

Home | Search | Data Bank | Data Services | Help

Search | All Words | e.g. 1606N020Q02

Please Sign In: You must sign in to your SAM.gov account to search Entities, Responsibility/Qualification and the Disaster Response Registry. | Sign In

Select Domain
Entity Information

All Entity Information

Entities

Disaster Response Registry

Responsibility / Qualification

Exclusions

Filter By

Keyword Search

For more information on how to use our keyword search, visit our help guide

Simple Search | Search Editor

- ( ) Any Words
- (•) All Words
- ( ) Exact Phrase

e.g. 123456789, Smith Corp

Deighton Associates LTD ×

Entity

Entity Name

No results found

Unique Entity ID

CAGE / NCAGE

Location

Status

- [x] Active
- [x] Inactive

Reset

No matches found

We couldn't find a match for your search criteria.

Please try another search or go back to previous results.

Go Back

COMPLIANCE VERIFICATION CHECKLIST
FOR REQUISITION SUBMISSION

Purchasing Division Use: Buyer: J. ESTEP Date: 12/18/24 Solicitation No. CMA DOT23*25 CO#3	Agency: WV DOT
	Procurement Officer Submitting Requisition: Kristy James
	Requisition No. CMA DOT23*25
	PF No.: 1119410

This checklist **MUST** be completed by a state agency's designated procurement officer and submitted with the Purchase Requisition to the Purchasing Division. The purpose of the checklist is to verify that an agency procurement officer has obtained and included required documentation necessary for the Purchasing Division to process the requisition without future processing disruptions. At the agency's preference, the agency **MUST** either submit the checklist by attaching it to the requisition's Header **OR** by placing it in the requisition's Procurement Folder.

FOR ALL SOLICITATION TYPES:

	Compliance Check Type	Required	Provided, if Required	Not Required	Purch. Div. Confirmation
1	Specifications and Pricing Page included	☑	☐	☐	☐
2	Use of correct specification template	☑	☐	☐	☐
3	Use of correct requisition type [CRQS → CCT or CPO] or [CRQM → CMA]	☑	☐	☐	☐
4	Use of most current terms and conditions (www.state.wv.us/admin/purchase/TCP.pdf)	☑	☐	☐	☐
5	Maximum budgeted amount in *wv*OASIS	☑	☐	☐	☐
6	Suggested vendors in *wv*OASIS	☑	☐	☐	☐
7	Capitol Building Commission pre-approval	☐	☐	☐	☐
8	Financing (Governor's Office) pre-approval	☐	☐	☐	☐
9	Fleet Management Division pre-approval	☐	☐	☐	☐

	Compliance Check Type	Required	Provided, if Required	Not Required	Purch. Div. Confirmation
10	Insurance requirements				
	Commercial General Liability	☐	☐	☐	☐
	Automobile Liability	☐	☐	☐	☐
	Workers' Compensation/Employer's Liability	☐	☐	☐	☐
	Cyber Liability	☐	☐	☐	☐
	Builder's Risk/Installation Floater	☐	☐	☐	☐
	Professional Liability	☐	☐	☐	☐
	Other (specify)	☐	☐	☐	☐
11	Office of Technology CIO pre-approval	☐	☐	☐	☐
12	Treasurer's Office (banking) pre-approval	☐	☐	☐	☐

FOR CHANGE ORDERS/RENEWALS:

1	Two-party agreement	☑	☐	☐	☑
2	Standard change order language	☑	☐	☐	☑
3	Office of Technology CIO approval	☐	☐	☑	☐
4	Justification for price increases/backdating/other	☐	☐	☑	☐
5	Bond Rider (Construction)	☐	☐	☑	☐
6	Secretary of State Verification	☑	☐	☐	☑
7	State debarment verification	☑	☐	☐	☑
8	Federal debarment verification	☑	☐	☐	☑

**The items pre-checked are required before a Purchase Requisition may be submitted to the Purchasing Division. Failure to complete and verify this documentation may result in rejection of the requisition back to the agency. It is up to the agency procurement officer to determine if pre-approvals, insurance, or other documentation is needed for the purchase. The referenced information below may be used to make this determination.*

For Purchasing Division Use Only:

I have reviewed the requisition identified above and find that it is sufficient to advertise publicly to the vendor community. My review does not preclude the possibility that the vendor community, or some other entity, will identify an area of concern; however, should such issues or concerns arise, they will be reviewed and addressed as may be appropriate.

Signature: _____