



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: 09-18-2024

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 0947 0947 ERP2500000001 2	Procurement Folder:	1376334
Document Name:	Identity Management Single Sign-On Solution	Reason for Modification:	Change Order No. 1 - to add Saas Addendum and attach a copy of the pricing pages for informational purposes only.
Document Description:	Identity Management Single Sign-On Solution		
Procurement Type:	Central Master Agreement		
Buyer Name:			
Telephone:			
Email:			
Shipping Method:	Best Way	Effective Start Date:	2024-09-01
Free on Board:	FOB Dest, Freight Prepaid	Effective End Date:	2027-08-31

VENDOR	DEPARTMENT CONTACT																				
Vendor Customer Code: 000000223330 DELL MARKETING LP ONE DELL WY ROUND ROCK TX 78682 US Vendor Contact Phone: 512-338-4400 Extension:	Requestor Name: Matthew H Ellison Requestor Phone: (304) 741-8565 Requestor Email: matt.ellison@wvoasis.gov																				
Discount Details:	2025 FILE LOCATION _____																				
<table><tr><th></th><th>Discount Allowed</th><th>Discount Percentage</th><th>Discount Days</th></tr><tr><td>#1</td><td>No</td><td>0.0000</td><td>0</td></tr><tr><td>#2</td><td>No</td><td></td><td></td></tr><tr><td>#3</td><td>No</td><td></td><td></td></tr><tr><td>#4</td><td>No</td><td></td><td></td></tr></table>			Discount Allowed	Discount Percentage	Discount Days	#1	No	0.0000	0	#2	No			#3	No			#4	No		
		Discount Allowed	Discount Percentage	Discount Days																	
#1		No	0.0000	0																	
#2		No																			
#3	No																				
#4	No																				

INVOICE TO	SHIP TO
CONTROLLER ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US	CONTROLLER ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US

9-18-24 6L

Purchasing Division's File Copy

Total Order Amount: Open End

PURCHASING DIVISION AUTHORIZATION
DATE: 9/19/24
ELECTRONIC SIGNATURE ON FILE

ATTORNEY GENERAL APPROVAL AS TO FORM
DATE: 9/25/2024
ELECTRONIC SIGNATURE ON FILE

ENCUMBRANCE CERTIFICATION
DATE: 9-25-24
ELECTRONIC SIGNATURE ON FILE

Extended Description:

Change Order No. 1 - to add the Saas Addendum to the contract that was inadvertently omitted from the original contract. Also, to attach a complete copy of the pricing page for informational purposes only.

No other changes.

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
1	81112501				0.000000
Service From		Service To		Service Contract Amount	
				0.00	

Commodity Line Description: Identity Management Single Sign-On Solution

Extended Description:

See attached documentation for complete details.

Version 11-1-19

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. One Identity has dedicated alternate data center locations in the U.S. and UK.

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 identity theft or other fraud.

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.

Version 11-1-19

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 that results 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,

Version 11-1-19

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.
- 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) 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 hosting 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

Version 11-1-19

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 or Data Breach as soon as practicable, but no later than forty-eight

(48) hours after the service provider becomes aware of it, to: email registered by customer on support.oneidentity.com. The following information shall be shared with the public jurisdiction and all affected customers: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity) only in certain cases as determined by provider, (2) projected business impact, and, (3) attack source information.

Any security incident or data breach specific to your entity only will be addressed to: 1) the department privacy officer, by email, identified in Appendix A.

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) The service provider may provide a contact 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.

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

Version 11-1-19

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 notifications to individuals, regulators or others required explicitly by state or federal law; a credit monitoring service if explicitly required by state or federal law; a website or a toll-free number and call center for affected individuals as 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) or the liability caps in the service provider's legal terms and conditions; and (5) complete all corrective actions as reasonably determined by service provider based on root cause.
- f) 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

Version 11-1-19

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.

In situations where the public jurisdiction takes actions under this subsection (f), service provider will have no further obligation to cover costs or other legal responsibilities, including remediation.

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 directly 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, unless prohibited by law from providing such notice. The service provider shall not respond to subpoenas, service of process and other legal requests directly 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 causeAfter 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, upon request. [Addressed in

Version 11-1-19

service provider's Software Transaction Agreement]

8. Background Checks: The service provider shall conduct criminal background checks in compliance with own defined policies, which can be provided upon request.

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. Security Logs and Reports: The service provider shall provide access 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: [Intentionally removed].

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

Version 11-1-19

systems and computing equipment, including, but not limited to, laptops 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 after a risk assessment has been completed, 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 its 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 terms and conditions consistent with applicable law.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to request that the service provider remove from interaction with public jurisdiction any service provider representative who the public jurisdiction believes is detrimental to

Version 11-1--19

its working relationship with the service provider.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery attestation letter upon request.

21. Compliance with Accessibility Standards: Provider documents the accessibility of its products as established by Section 508 Amendment to the Rehabilitation Act of 1973 and publishes the resulting VPAs at <https://oneidentity.com/legal/section-508.aspx>.

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 as set forth in its Software Transaction Agreement.

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 and service provider's Software Transaction Agreement to the contrary.

26. Any Software is licensed on the terms and conditions of the Software Transaction Agreement ("STA") located at <https://www.oneidentity.com/legal/sta.aspx> as of the date of the initial license, and this Software as a Service Addendum will become an Addendum to the STA.

27. Nothing in this Addendum shall negate or be construed to negate the applicability of WV Code §5A-3-62, which set forth those terms and conditions which are automatically void under West Virginia State Law, including but not limited to, the applicability generally of West Virginia Law for this and all other agreements entered into with the State of West Virginia.

Version 11-1-19

AGREED:

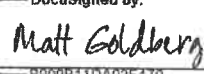
Name of Agency: WV ERP BOARD

Signature: 
EVAN PAVLOV

Title: CONTROLLER

Date: 9/16/2024

Name of Vendor One Identity LLC

Signature: 
DocuSigned by:
B909B11DA02E470...

Title: Head of Legal

Date: 9/18/2024

Exhibit A - Pricing Page				
Identity Management Single Sign-On Solution Licensing				
	Description	Unit Price	Quantity	Extended Price (Annual Price)
Year 1	SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month(**)	\$7,252.11	12	\$87,025.32
Year 2	SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month(**)	\$7,252.11	12	\$87,025.32
Year 3	SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month(**)	\$7,252.11	12	\$87,025.32
Optional Year 4	SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month(**)	\$7,900.00	12	\$94,800.00
Optional Year 5	SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month(**)	\$8,700.00	12	\$104,400.00
Optional Year 6	SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month(**)	\$9,580.00	12	\$114,960.00
	Additional Unique Logins by User (per month)(**)	\$5.76	1,000	\$5,760.00
	SAAS Monthly Support (If necessary)		12	\$0.00
Subtotal (Section A) Licensing				\$580,995.96

Support and Implementation Services						
	Title	Estimated Quantity (Onsite)	Onsite Hourly Rate(***)	Estimated Quantity (Offsite)	Offsite Hourly Rate	Extended Price
	Services and Support to include Data Conversion		\$329.03		\$329.03	\$39,483.60
Subtotal (Section B) Support and Implementation Services						\$39,483.60
TOTAL BID AMOUNT (Sum of Section A and B)						\$620,479.56
*All pricing includes travel charges. Quantities are estimates for evaluation purposes only						

ALTERNATE PRICING FOR ADDITIONAL EXTERNAL USERS				
	Description	Unit Price	Quantity	Extended Price (Annual Price)
Year 1	External Users (6,000)	\$1,902.67	12	\$22,832.04
Year 2	External Users (6,000)	\$1,902.67	12	\$22,832.04
Year 3	External Users (6,000)	\$1,902.67	12	\$22,832.04
Optional Year 4	External Users (6,000)	\$2,075.00	12	\$24,900.00
Optional Year 5	External Users (6,000)	\$2,285.00	12	\$27,420.00
Optional Year 6	External Users (6,000)	\$2,510.00	12	\$30,120.00
Subtotal (Section A) Licensing				\$150,936.12

NOTES: (**)(***)

We appreciate the opportunity to clarify certain aspects of our licensing model. We need to clarify that our Monthly Active User licensing model is strictly reserved for Customer Identity & Access Management (CIAM). There are no internal or external variations of this model; it's specifically for unique monthly active users from a CIAM perspective,

(**)

whether they are B2C or B2B users.



Lyle, Tara L <tara.l.lyle@wv.gov>

Fwd: CRFP # 0947 ERP24*02

1 message

Willis, Samantha L <samantha.l.willis@wv.gov>

Fri, Sep 13, 2024 at 12:32 PM

To: Frank M Whittaker <frank.m.whittaker@wv.gov>, Tara L Lyle <tara.l.lyle@wv.gov>, Larry D McDonnell <larry.d.mcdonnell@wv.gov>

Would you guys please coordinate with ERP to get this signed on our end so we can finalize and add through a change order?

Thanks!

----- Forwarded message -----

From: **Matt Goldberg (mgoldber)** <Matt.Goldberg@oneidentity.com>

Date: Wed, Sep 11, 2024 at 5:30 PM

Subject: Re: CRFP # 0947 ERP24*02

To: Willis, Samantha L <samantha.l.willis@wv.gov>, David Schwab (dschwab) <David.Schwab@oneidentity.com>

Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>, Larry D McDonnell <larry.d.mcdonnell@wv.gov>, Michelle Lewis (mlewis) <Michelle.Lewis@quest.com>

All good from our side... How do you want to process this document?

Matt Goldberg

One Identity | Legal

From: Willis, Samantha L <samantha.l.willis@wv.gov>

Sent: Wednesday, September 11, 2024 1:58 PM

To: David Schwab (dschwab) <David.Schwab@oneidentity.com>

Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>; Matt Goldberg (mgoldber) <Matt.Goldberg@quest.com>

Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

Please find attached the updated PDF of the document ready for execution. Let me know if you identify any errors or omissions.

Thanks,
Sam

On Tue, Sep 10, 2024 at 3:19 PM Willis, Samantha L <samantha.l.willis@wv.gov> wrote:

Apologies for the delay I had intended to respond to this yesterday. I will make these changes and get an updated version to you first thing tomorrow morning.

Thank you again!
Sam

Samantha Willis
Director & General Counsel
Purchasing Division
304-558-0492 • Samantha.L.Willis@wv.gov



On Tue, Sep 10, 2024 at 2:20 PM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

Hi Samantha,

I meant to copy in Matt last night but see I did not. Hopefully that will help us speed up the process.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

-

www.oneidentity.com



From: David Schwab (dschwab) <David.Schwab@oneidentity.com>
Sent: Monday, September 9, 2024 7:01 PM
To: Willis, Samantha L <samantha.l.willis@wv.gov>
Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>
Subject: RE: CRFP # 0947 ERP24*02

Hi Samantha,

Feedback from Matt:

we are okay including that W.Va. statute insert.

However, I did not see a final document from them. Please ask Samantha to check my comments in Section 7 for cleanup, and also confirm that the Background insert will be only as follows:

The service provider shall conduct criminal background checks in compliance with own defined policies, which can be provided upon request.

I am available this week if she has any final questions on the document.

Matt

Matt Goldberg

One Identity | Legal

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

-

www.oneidentity.com



From: Willis, Samantha L <samantha.l.willis@wv.gov>

Sent: Monday, September 9, 2024 5:15 PM

To: David Schwab (dschwab) <David.Schwab@oneidentity.com>

Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>

Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

Great news David! Thanks so much!

On Mon, Sep 9, 2024 at 2:28 PM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

Hi Samantha,

We are just waiting for one final approval from our CFO and I expect an answer by end of day or early Tuesday.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: Willis, Samantha L <samantha.l.willis@wv.gov>

Sent: Friday, September 6, 2024 6:41 AM

To: David Schwab (dschwab) <David.Schwab@oneidentity.com>

Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>

Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

Thank you David, much appreciated!

Samantha Willis
Director & General Counsel
Purchasing Division
304-558-0492 • Samantha.L.Willis@wv.gov



On Thu, Sep 5, 2024 at 4:08 PM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

Hi Samantha,

I just wanted to let you know we are still working through that final clause on the SaaS form. We will keep you updated.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: Willis, Samantha L <samantha.l.willis@wv.gov>

Sent: Tuesday, September 3, 2024 2:52 PM

To: David Schwab (dschwab) <David.Schwab@oneidentity.com>

Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>

Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

Thank you very much! I will speak to you all tomorrow then!

On Tue, Sep 3, 2024 at 2:36 PM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

Great and thank you Sam. I just sent an invite for 4 PM EST Wednesday. Please add whomever you want to include.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: Willis, Samantha L <samantha.l.willis@wv.gov>

Sent: Tuesday, September 3, 2024 2:05 PM

To: David Schwab (dschwab) <David.Schwab@oneidentity.com>

Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>

Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

David,

I would be happy to hop on a call with Mr. Goldberg to nail down the final details. I am available after 3pm tomorrow, and all day Friday.

Thanks!

Sam

On Sat, Aug 31, 2024 at 9:53 AM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

Hi Samantha,

Attached please find out feedback from our legal. Matt Goldberg wanted to also offer to hold a call to finalize this if that makes sense. Have a great holiday weekend.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: David Schwab (dschwab) <David.Schwab@oneidentity.com>
Sent: Thursday, August 29, 2024 10:13 AM
To: Willis, Samantha L <samantha.l.willis@wv.gov>
Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>
Subject: RE: CRFP # 0947 ERP24*02

Thank you so much Samantha. I will pass along to our legal team and advise them of your offer for a call, which is very helpful as well.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: Willis, Samantha L <samantha.l.willis@wv.gov>
Sent: Thursday, August 29, 2024 10:06 AM
To: David Schwab (dschwab) <David.Schwab@oneidentity.com>
Cc: Frank M Whittaker <frank.m.whittaker@wv.gov>; Larry D McDonnell <larry.d.mcdonnell@wv.gov>
Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

David,

Please find attached my suggested revisions to your team's redlines. I would be more than happy to hop on a call today or tomorrow to discuss this with your legal team.

Best,

Sam

On Tue, Aug 27, 2024 at 12:35 PM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

OK great and thank you.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: Willis, Samantha L <samantha.l.willis@wv.gov>

Sent: Tuesday, August 27, 2024 12:32 PM

To: David Schwab (dschwab) <David.Schwab@oneidentity.com>

Subject: Re: CRFP # 0947 ERP24*02

CAUTION: This email originated from outside of the organization. Do not follow guidance, click links, or open attachments unless you recognize the sender and know the content is safe.

Thank you for reaching out David. I will be looking over your redlines today and providing feedback this afternoon.

Sam

On Tue, Aug 27, 2024 at 11:21 AM David Schwab (dschwab) <David.Schwab@oneidentity.com> wrote:

Hi Samantha,

We returned a redline of the SaaS form to Larry & Tara and wanted to see if you knew the current status? Our legal team is happy to hold a call with you to discuss.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



From: David Schwab (dschwab)
Sent: Friday, August 2, 2024 11:12 AM
To: samantha.l.willis@wv.gov
Subject: CRFP # 0947 ERP24*02

Hi Samantha,

I wanted to reach out to let you know I am your account rep for One Identity for this RFP. I know Dell was providing additional documentation and please feel free to reach out to me if you need anything from One Identity.

Best Regards,

David Schwab

Account Executive, Mid-Atlantic



M: 610-304-6444

E: david.schwab@quest.com

www.oneidentity.com



Samantha Willis
Director & General Counsel
Purchasing Division
304-558-0492 • Samantha.L.Willis@wv.gov



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. One Identity has dedicated alternate data center locations in the U.S. and UK.

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 identity theft or other fraud.

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 that results 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.
- 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) 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 hosting 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 or Data Breach as soon as practicable, but no later than forty-eight

(48) hours after the service provider becomes aware of it, to: email registered by customer on support.oneidentity.com. The following information shall be shared with the public jurisdiction and all affected customers: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity) only in certain cases as determined by provider, (2) projected business impact, and, (3) attack source information.

Any security incident or data breach specific to your entity only will be addressed to: 1) the department privacy officer, by email, identified in Appendix A.

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) The service provider may provide a contact 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.

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 notifications to individuals, regulators or others required explicitly by state or federal law; a credit monitoring service if explicitly required by state or federal law; a website or a toll-free number and call center for affected individuals as 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) or the liability caps in the service provider's legal terms and conditions; and (5) complete all corrective actions as reasonably determined by service provider based on root cause.
- f) 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.

In situations where the public jurisdiction takes actions under this subsection (f), service provider will have no further obligation to cover costs or other legal responsibilities, including remediation.

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 directly 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, unless prohibited by law from providing such notice. The service provider shall not respond to subpoenas, service of process and other legal requests directly 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 causeAfter 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, upon request. [Addressed in

service provider's Software Transaction Agreement]

8. Background Checks: The service provider shall conduct criminal background checks in compliance with own defined policies, which can be provided upon request.

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. Security Logs and Reports: The service provider shall provide access 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: [Intentionally removed].

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, laptops 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 after a risk assessment has been completed, 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 its 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 terms and conditions consistent with applicable law.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to request 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.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery attestation letter upon request.

21. Compliance with Accessibility Standards: Provider documents the accessibility of its products as established by Section 508 Amendment to the Rehabilitation Act of 1973 and publishes the resulting VPAs at <https://oneidentity.com/legal/section-508.aspx> .

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 as set forth in its Software Transaction Agreement.

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 and service provider's Software Transaction Agreement to the contrary.

26. Any Software is licensed on the terms and conditions of the Software Transaction Agreement ("STA") located at <https://www.oneidentity.com/legal/sta.aspx> as of the date of the initial license, and this Software as a Service Addendum will become an Addendum to the STA.

27. Nothing in this Addendum shall negate or be construed to negate the applicability of WV Code §5A-3-62, which set forth those terms and conditions which are automatically void under West Virginia State Law, including but not limited to, the applicability generally of West Virginia Law for this and all other agreements entered into with the State of West Virginia.

AGREED:

Name of Agency: _____

Name of Vendor _____

Signature: _____

Signature: _____

Title: _____

Title: _____

Date: _____

Date: _____

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.

DELL MARKETING L P

Organization Information								
Org Type	Effective Date	Established Date	Filing Date	Charter	Class	Sec Type	Termination Date	Termination Reason
GP General Partnership	1/7/1999			Domestic				

Organization Information		
Business Purpose	Capital Stock	
Charter County	Control Number	
Charter State	WV	Excess Acres
At Will Term	Member Managed	
At Will Term Years	Par Value	
Authorized Shares	Young Entrepreneur	Not Specified



Addresses	
Type	Address
Mailing Address	1 DELL WAY MS RR1-38 ROUND ROCK, TX, 786829256
Principal Office Address	1 DELL WAY MS RR1-38 ROUND ROCK, TX, 786829256
Type	Address

Officers	
Type	Name/Address
Partner	DELL MARKETING L P 1 DELL WAY MS RR1-38 ROUND ROCK, TX, 786829256
Type	Name/Address

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

Wednesday, September 18, 2024 — 2:20 PM

© 2024 State of West Virginia



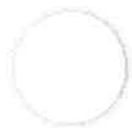
Addresses	
Type	Address
Mailing Address	1 DELL WAY MS RR1-38 ROUND ROCK, TX, 786829256
Principal Office Address	1 DELL WAY MS RR1-38 ROUND ROCK, TX, 786829256
Type	Address

Officers	
Type	Name/Address
Partner	DELL MARKETING L P 1 DELL WAY MS RR1-38 ROUND ROCK, TX, 786829256
Type	Name/Address

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

Wednesday, September 18, 2024 — 2:20 PM

© 2024 State of West Virginia



Keyword Search

For more information on how to use our keyword search, visit our help guide [\[?\]](#)

Simple Search

Search Editor

- ☐ Any Words i
- ☒ All Words i
- ☐ Exact Phrase i

e.g. 123456789, Smith Corp

"dell marketing lp" ×

Entity ▼

Location ▼

Status ^

- ☒ Active
- ☐ Inactive

Reset ↺



No matches found

Your search did not return any results for active records.

Would you like to include inactive records in your search results?

Search inactive

Go back

COMPLIANCE VERIFICATION CHECKLIST FOR REQUISITION SUBMISSION

Purchasing Division Use:		Agency:
Buyer: <u>R</u>	Date: <u>9/18/24</u>	WV ERP
Solicitation No. <u>CO#1</u>		Procurement Officer Submitting Requisition:
		Evan Pauley
		Requisition No.
		CMA ERP25*01 - CO#1
		PF No.:
		1376334

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Use of correct specification template	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Use of correct requisition type [CRQS → CCT or CPO] or [CRQM → CMA]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Use of most current terms and conditions (www.state.wv.us/admin/purchase/TCP.pdf)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	Maximum budgeted amount in wvOASIS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Suggested vendors in wvOASIS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	Capitol Building Commission pre-approval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	Financing (Governor's Office) pre-approval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	Fleet Management Division pre-approval	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

FOR CHANGE ORDERS/RENEWALS:

1	Two-party agreement	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Standard change order language	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Office of Technology CIO approval	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	Justification for price increases/backdating/other	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Bond Rider (Construction)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	Secretary of State Verification	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	State debarment verification	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	Federal debarment verification	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

*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: Tara Hef