

## STATE OF ILLINOIS CONTRACT

Department of Innovation and Technology  
JPMC Dell Server and Storage Solutions  
CMT4040325

---

The Parties to this Contract are the State of Illinois acting through the Department of Innovation and Technology (the State or DoIT) and AHEAD, Inc. (Vendor). This Contract (also referred to as the “State Terms”), consisting of the signature page and numbered sections listed below and any attachments referenced and included herein, constitute the entire Contract between the Parties concerning the subject matter of the Contract, and in signing the Contract, the Vendor affirms that the Certifications and Financial Disclosures and Conflicts of Interest attached hereto are true and accurate as of the date of the Vendor’s execution of the Contract. This Contract supersedes all prior proposals, contracts and understandings between the Parties concerning the subject matter of the Contract. This Contract can be signed in multiple counterparts upon agreement of the Parties.

Contract includes BidBuy Purchase Order? (The Agency answers this question prior to Contract filing.)

Yes

No

Contract uses Illinois Procurement Gateway Certifications and Disclosures?

Yes (IPG Certifications and Disclosures including IPG Active Registered Vendor Disclosure formerly named Forms B)

No

1. **DESCRIPTION OF SUPPLIES AND SERVICES**
2. **PRICING**
3. **TERM AND TERMINATION**
4. **STANDARD BUSINESS TERMS AND CONDITIONS**
5. **STATE SUPPLEMENTAL PROVISIONS**
6. **STANDARD ILLINOIS CERTIFICATIONS**
7. **FINANCIAL DISCLOSURES AND CONFLICTS OF INTEREST**
8. **CONTRACT SPECIFIC CERTIFICATIONS AND DISCLOSURES – “IPG Active Registered Vendor Disclosure (formerly called FORMS B)” (IF APPLICABLE)**
9. **PURCHASE ORDER FROM BIDBUY (IF APPLICABLE)**

**STATE OF ILLINOIS  
CONTRACT**

Department of Innovation and Technology  
JPMC Dell Server and Storage Solutions  
CMT4040325

---

Related terms entered into between the State and manufacturer Dell Marketing L.P. (“Dell”) are also attached to this Contract for reference (together, the “Dell Terms”) as follows:

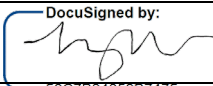
- The Dell Commercial Terms of Sale (“CTS”);
- Exhibit A: the Dell Software End User License Agreement (“EULA”);
- Exhibit B: the Dell Cloud Service Offerings Agreement (“CSOA”);
- Exhibit C: the Dell Cloud Services Data Processing Addendum (“DPA”);
- Exhibit D: the Dell APEX Subscriptions Terms for Partner End Users-US Public (“APEX-Subscriptions”); and
- Exhibit E: the Dell Privacy Statement—United States (“Privacy Statement”).

In consideration of the mutual covenants and agreements contained in this Contract, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree to the terms and conditions set forth herein and have caused this Contract to be executed by their duly authorized representatives on the dates shown on the following CONTRACT SIGNATURES page

**STATE OF ILLINOIS  
CONTRACT**

Department of Innovation and Technology  
JPMC Dell Server and Storage Solutions  
CMT4040325

**VENDOR**

Vendor Name: Ahead, Inc.	Address (Street/City/State/Zip): 444 W. Lake St., Suite 3000, Chicago, IL 60606
Signature:  <small>DocuSigned by: 50C7B34859B7475...</small>	Phone:
Printed Name: Mark Killian	Fax:
Title: Chief Financial Officer	ALL NOTICES TO: Email: legal@ahead.com
Date: 4/7/2025	

**STATE OF ILLINOIS**

Procuring Agency: Department of Innovation and Technology	Phone:
Street Address: 120 W. Jefferson Street	Fax:
City, State ZIP: Springfield, IL 62702	ALL NOTICES TO: Email: <a href="mailto:DoIT.ITPO.Communications@Illinois.gov">DoIT.ITPO.Communications@Illinois.gov</a> and <a href="mailto:DoIT.GeneralCounsel@Illinois.gov">DoIT.GeneralCounsel@Illinois.gov</a>
Official Signature: 	Date: 4/18/2025
Printed Name: Brandon Ragle	
Official's Title: Acting Secretary	
Legal Signature: 	Date: 04/18/2025
Legal Printed Name: Radhika Lakhani	
Legal's Title: General Counsel	
Fiscal Signature: 	Date: 04/17/2025
Fiscal's Printed Name: Mary Feagans	
Fiscal's Title: Chief Fiscal Officer	

**AGENCY USE ONLY**

**NOT PART OF CONTRACTUAL PROVISIONS**

- Agency Reference #: 25-448DOIT-INFOT-B-43199
- Project Title: JPMC Dell Server and Storage Solutions
- Contract #: CMT4040325
- Procurement Method (IFB, RFP, Small Purchase, etc.): IFB
- BidBuy / Bulletin Reference #: 25-448DOIT-INFOT-B-43199
- BidBuy / Bulletin Publication Date:
- Award Code: A
- Subcontractor Utilization?  Yes  No      Subcontractor Disclosure?  Yes  No
- Funding Source:
- Obligation #:
- Small Business Set-Aside?  Yes  No      Percentage:
- Minority Owned Business?  Yes  No      Percentage: 5%
- Women Owned Business?  Yes  No      Percentage:
- Persons with Disabilities Owned Business?  Yes  No      Percentage:
- Veteran Owned Small Business?  Yes  No      Percentage:
- Other Preferences?

## 1. DESCRIPTION OF SUPPLIES AND SERVICES

1.1. **GOAL:** DoIT, in cooperation and agreement with the Chief Procurement Officer for General Services, hereby executes a multi-year indefinite quantity, Joint Purchase Master Contract (JPMC) with Vendor, a Dell solution provider, for purchase of Dell brand servers and storage (non-cloud-based and cloud-based), accessories, replacement and upgrade components, installation and configuration services, maintenance and support services, professional services and cloud server and storage solutions to be available to all governmental units and qualified not-for-profit agencies. However, of the full range of products and services available under this Contract, DoIT is **only** authorized to purchase cloud-based products and services. On the other hand, for any purchase of the non-cloud-based products and services otherwise available under this Contract, DoIT will continue to utilize its pre-existing contract # CIT9422100 (P-5839). Note: Any State order for cloud-based offerings will be subject to a Cloud Storage Area within the contiguous United States, as provided in the Dell Terms (specifically, see Section 12 (“Data Privacy”) of the CTS and Sections 1 (“Definitions”—defining the term “Cloud Storage Area”) & 12.2 (“Data Processing”) of the CSOA, Exhibit B to the CTS).

To ensure compatibility and proper functionality within the State’s infrastructure, only Dell brand products and services will satisfy the State’s needs, no other brands’ products and services will be considered.

1.2. **SUPPLIES AND/OR SERVICES REQUIRED:** Vendor will continue to be an authorized Dell solution provider through the term of this Contract, and will accept orders under this Contract for the purchase of Dell brand servers and storage (non-cloud-based and cloud-based), accessories, replacement and upgrade components, installation and configuration services, maintenance and support services, professional services and cloud server and storage solutions to be available to all governmental units and qualified not-for-profit agencies. These products and services are as defined and specified in the subsections below.

1.2.1 Dell Brand Servers, Non-Cloud-Based (Non-Cloud-Based Servers) include but are not limited to: Dell PowerEdge Tower; Dell PowerEdge Servers; Dell PowerEdge Modular Infrastructure; Dell PowerEdge Blade; Dell Precision; VX Rail Package and Dell PowerEdge C-Series.

1.2.2 Dell Brand Storage, Non-Cloud-Based (Non-Cloud-Based Storage Products) include but are not limited to: Dell PowerVault; Dell Unity; Dell SC Series; Dell PowerMax; and Dell Data Domain. These products are available in different form factors, including as: Network-Attached Storage (NAS), Storage Area Network (SAN), and Direct Attached Storage (DAS) options, to suit different storage requirements.

- 1.2.3 Dell Server and Storage Accessories (Accessories) refer to components, peripherals, or add-ons that can be used to enhance or expand the functionality of Dell servers and storage systems. Accessories are designed to work with Dell server and storage solutions, providing additional features, capabilities, or convenience for users. Some common Accessories include but are not limited to: Rack Mount Kits; Network Interface Cards (NICs); Fiber Optic Transceivers; Switches; Cables and Connectors; Network Management Software; and Network Security Appliances. Dell offers a wide range of Accessories to enhance networking capabilities and provide a solution for server and storage infrastructure within a network environment.
- 1.2.4 Dell Server and Storage Replacement and Upgrade Components (Replacement and Upgrade Components) refer to the individual parts, modules, or components that can be used to replace or upgrade specific hardware elements within Dell servers and storage systems. Replacement and Upgrade Components are designed to be compatible with Dell's infrastructure, ensuring integration and performance. Some common Replacement and Upgrade Components include but are not limited to: Processors (CPU); Memory Modules (RAM); Hard Drives and Solid-State Drives; RAID Controllers; Power Supplies; Network Adapters; and Cooling Fans. Dell provides a wide range of such components that can be used to replace or upgrade specific hardware elements within servers and storage systems, allowing users to customize their infrastructure according to their needs.
- 1.2.5 Dell Server and Storage Installation and Configuration Services (Installation and Configuration Services) include professional services required for the set up and configuration of Dell servers and storage systems. Some Installation and Configuration Services include but are not limited to: Site Assessment; Hardware Installation; Remote Installation; Operating System Installation; Storage Configuration; Network Configuration; Data Migration; System Integration; Testing and Validation; and Training and Knowledge Transfer. The specific services available vary depending on the product and Agency requirements. Vendor shall provide Installation and Configuration Services at the job description hourly rates listed within the Bid Buy system under the Items Tab on an as needed, if needed, basis and at the State's request. Installation and Configuration Services work efforts will require a SOW with responsible parties, hourly rates, defined deliverables and/ or task milestones identified that will be completed. The SOW must be submitted along with the quote.
- 1.2.6 Dell Server and Storage Maintenance and Support Services (Maintenance and Support Services) are ongoing services provided to ensure the proper functioning and performance of Dell server and storage systems throughout their life cycle. These services are designed to assist agencies with maintaining IT infrastructure, minimizing downtimes, and maximizing the return on investment for Dell server and storage systems. Maintenance and Support Services include but are not limited to: Hardware Maintenance; Software Support; Proactive Monitoring of server and storage systems to identify potential issues before causing downtime

and performance degradation includes remote monitoring tools that track server and storage systems health, performance metrics, and alert notifications; Technical Support including phone support, online chat, or email support providing guidance, troubleshooting assistance, and recommendations; Patch Management; Spare Parts Management; Escalation Management; and Knowledge Base and Self-Service Resources. Maintenance and Support Services as well as level 1 services generally will not require a SOW, except that any specific custom Services efforts will require a SOW with responsible parties, hourly rates, defined deliverables and/ or task milestones identified that will be completed. For any such specific custom Services efforts, the SOW should be submitted along with the quote.

1.2.7 Dell Server and Storage Professional Services (Professional Services) provide development, implementation, integration, and advisory services for server and storage solutions. Professional Services work efforts will require a SOW with responsible parties, hourly rates, defined deliverables and/ or task milestones identified that will be completed. The SOW must be submitted along with the quote.

A) Dell Server and Storage Development Services (Development Services) assist agencies in the design development, and implementation of customized server and storage solutions. These services include but are not limited to: Consultation and Needs Assessment; Solution Design and Architecture; Hardware Configuration and Integration; Software and Operating System Integration; Performance Testing and Optimization of Server and Storage Systems; Data Migration and Storage Management; Training and Knowledge Transfer; and Ongoing Support and Maintenance. Development Services assist with customized solutions that address specific agencies needs and objectives. These services are designed to assist with IT infrastructure, improve performance, scalability, and reliability to achieve the agencies goals.

B) Dell Server and Storage Implementation Services (Implementation Services) assist agencies in the deployment and installation of Dell server and storage solutions. These services assist with the implementation of hardware, software, and networking components required for agencies infrastructure. Implementation Services include but are not limited to: Project Planning and Management; Hardware Procurement and Configuration; Software Installation and Configuration; Network Integration and Connectivity; Data Migration and Storage Setup; Testing and Validation; Training and Knowledge Transfer; and Documentation and Handover. Implementation Services assist with the deployment of Dell hardware and software solutions. These services assist with the IT infrastructure, minimize downtime, ad maximize performance and reliability of agencies' server and storage systems.

C) Dell Server and Storage Integration Services (Integration Services) assist agencies with integrating Dell server and storage solutions into the agencies' existing IT infrastructure. These services are designed to ensure

that the server and storage systems work together effectively, efficiently, and in alignment with the agencies specific requirements. Integration Services include but are not limited to: Infrastructure Assessment; Solution Design and Architecture; Hardware and Software Configuration; Network Integration and Connectivity; Data Migration and Storage Consolidation; System Testing and Validation; Training and Knowledge Transfer; and Ongoing Support and Maintenance. Integration Services aim to streamline the integration process, minimize disruption, and maximize integrated infrastructure.

- D) Dell Server and Storage Advisory Services (Advisory Services) provide guidance and recommendations to agencies regarding their server and storage infrastructure. These services are designed to assist agencies to make informed decisions, optimize their IT infrastructure, and align agency server and storage solutions with the agencies' goals and requirements. Advisory Services include but are not limited to: Needs Assessment; Solution Design and Architecture; Technology Evaluation and Selection; Performance Optimization; Capacity Planning; Data Management and Protection; Security and Compliance; and Technology Roadmap. These services aim to assist agencies with guidance and recommendations to optimize server and storage infrastructure.

1.2.8 Dell Cloud Server and Storage Solutions (Cloud Server and Storage Solutions) include but are not limited to: Dell Cloud Manager; Dell Cloud Solutions: including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) options; Dell Cloud Client Computing; Dell Cloud Storage: including object storage, file storage, and block storage options; and Dell Cloud Networking: including switches, routers, and software-defined networking (SDN) solutions. Cloud Server and Storage solutions can support and enable a wide range of possible uses, including but not limited to example uses such as: mobile videos, body cams, body cam footage storage, dash cam footage storage, other public safety data such as video footage from drones, mobile devices and in car cameras, big data and analytics, artificial intelligence data, virtualized environments, data protection and back up, file and object storage and high-performance computing. To qualify as a Cloud Server and Storage Solution under this Contract, an offered solution must have the following features:

- a) Large Storage Capacity: provide storage space to accommodate storage uses such as the above list of examples, ensuring that agencies can store and access their data without running out of storage space.
- b) Secure Data Storage: employ encryption techniques to protect the stored data from unauthorized access and ensure data privacy. Security is a crucial aspect of cloud storage, including for the example storage uses listed above.
- c) Easy Accessibility: allow users to access their data from anywhere, at any time, using various devices such as smartphones, tablets, and computers. This enables remote access and collaboration among team

members.

- d) Scalability: provide the ability to scale up or down based on agencies' needs, including flexibility to adjust storage capacity as the volume of data increases or decreases.
- e) Data Backup and Recovery: allow the ability to automatically back up data to ensure the data is protected against accidental deletion, device loss, or damage. In case of any data loss, agencies can then easily recover their data from the cloud storage.
- f) Integration with Video Management Systems (VMS): offer the ability to integrate with VMS or other video analytics platforms. The integration enables video storage, retrieval, and analysis, enhancing the video management process.
- g) Compliance and Data Governance: adhere to industry regulations, as defined in the State of Illinois Security terms and conditions, and State of Illinois data protection laws by providing features like audit logs, access controls, and data retention policies to ensure compliance and data governance.
- h) Real-time Streaming and Sharing: enable real-time streaming and sharing of data. This allows authorized personnel to view and share data instantly, improving collaboration and decision-making processes.
- i) Cloud Storage for Law Enforcement Agencies: shall have to meet the current version, and all subsequent versions, of the Federal Bureau of Investigations' Criminal Justice Information Service Security Policy. The current version as of the effective date of this Contract is v5.9.1 published 10/1/22, but may be updated thereafter.
- j) For further clarity, Dell Brand Servers, Cloud-Based (Cloud-Based Servers) include but are not limited to: Dell PowerEdge Server; Dell PowerEdge Modular Infrastructure; Dell PowerEdge Racks; VX Rail Package, Dell PowerEdge C-Series; Dell PowerEdge VRTX; and Dell PowerOne.
- k) For further clarity, Dell Brand Storage, Cloud-Based (Cloud-Based Storage Solutions) include but are not limited to: Dell PowerStore; Dell PowerScale; Dell ECS (Elastic Cloud Storage); Dell Isilon; and Dell Cloud Storage Services, and Dell Cloud Storage with Virtustream.

1.2.9 All products furnished shall be new, unused, and most recent manufacture and not discontinued. Given the changing marketplace and the evolution of technology, the State, during any term of the contract, may review new and enhanced products, maintenance and support services, or equipment offered by Vendor that are within the scope of the contract and underlying procurement. In addition, if an item becomes discontinued or otherwise not available during any term, Vendor may propose to substitute an equivalent or better product. Prices

and rates for any product or service offered may be revised downward from the Contract price, but not upward. Similarly, discount schedules may be increased from the original Contract, but not decreased. Any new technology the State takes advantage of must, at a minimum, replace a function or solution that the Contract already covers.

- 1.2.10 Vendor shall include in each quote Dell's three (3) year minimum industry standard warranty and Maintenance and Support Services coverage for orders of applicable Dell offerings, as described in the Dell Terms attachments to this Contract, unless the State chooses to purchase a higher level or longer-term period of such warranty or Maintenance and Support Services coverage (or otherwise extend any existing warranty or Maintenance and Support Services coverage).
- 1.2.11 This Contract includes as attachments any license agreement(s) or additional terms and conditions that govern the use of the software or other services or supplies.
- 1.2.13 Vendor may incorporate additions to their Dell offerings within the scope of products and services categories as listed and described herein. The MSRP pricelist may be updated with additional Dell offerings when they become available by submitting a written request to DoIT via email DoIT.ITPO.Communications@Illinois.gov. Any proposed additions to Vendor's Dell offerings must be approved by DoIT prior to their inclusion within the MSRP pricelist.
- 1.2.14 Any Vendor terms and conditions on Vendor's ordering document(s) shall not apply to the Contract or any orders against it. Nothing in this Contract or elsewhere, including in any non-State approved forms, shall create any obligation to purchase, and make payments on, any products or services offered hereunder.
- 1.2.15 The State shall have no minimum purchase obligation or minimum order requirement under this Contract. Orders against this Contract will be made by the State using a State-approved form (e.g. a Basic Ordering Agreement (BOA), together with a SOW where required) on an as needed, if needed, basis. All governmental units and qualified not-for-profit agencies will submit their own purchase forms. Orders written through and including the last day of the Contract shall be honored. This excludes orders for services, as no services may extend past the last day of the resulting contract (other than normal prepaid annual maintenance). Each individual order will have its own ship to/bill to information.
- 1.2.16 Vendor, either directly or in collaboration with manufacturer, shall provide the State a copy of the SOC2 report related to any cloud subscriptions for State review and approval.

For procurements conducted in Bid Buy, the State may include in this Contract the Bid Buy Purchase Order as it contains the agreed Supplies and/or Services.

**1.3. MILESTONES AND DELIVERABLES:**

- 1.3.1. Milestones and Deliverables shall be addressed in a SOW to be included, where required, with orders against this Contract.
- 1.3.2. Vendor shall provide usage reports at the beginning of each quarter (quarter is a period of 3 months beginning with July) detailing the equipment, services and costs of orders placed against this contract during the previous quarter.
- 1.3.3. Vendor shall provide annually during the month of July, a compiled list of each usage report from the previous State Fiscal Year.
- 1.3.4. Vendor's Manufacturer Suggested Retail Pricing (MSRP) Price List is attached to this Contract, and is subject to the provisions of Section 2.1.6.

**1.4. VENDOR / STAFF SPECIFICATIONS:**

- 1.4.1 Vendor is and shall remain a Dell Solutions Partner authorized to resell or perform installation and configuration services on Dell products throughout the term of this contract. DoIT is aware that, in the IT industry, manufacturers often make products or services available to customers via an indirect channel. Those channel participants may be referred to as resellers, distributors, partners, providers or other designations.
- 1.4.2 Vendor staff positions, listed in Section 2 of this Contract, shall possess Dell Certification within the job requirements of the position.

**1.5. TRANSPORTATION AND DELIVERY:**

- 1.5.1. Transportation and Delivery and/or electronic delivery shall be as stated on each individual order.
- 1.5.2. Delivery will be made F.O.B. Destination, where transportation and physical delivery is applicable, with all transportation and handling paid by Vendor and charged back to any Governmental Unit or Qualified Not-For-Profit Agency location within the State of Illinois. Delivery locations will be identified on individual orders. Vendor shall coordinate delivery location requirements with ordering entity prior to shipment. There is no minimum for F.O.B Destination. Freight bill must be submitted with invoice.
- 1.5.3. Delivery including electronic delivery shall be made five (5) business days following order placement as directed by the ordering entity concerned unless other delivery terms have been agreed to by the ordering entity and Vendor. It shall be the responsibility of Vendor to contact the ordering entity directly for exact virtual or shipping and arrival dates and other operating instructions. The contact's name and telephone number should be listed on each order.

- 1.5.4. Prior to delivery, Vendor shall ensure delivery company or driver must contact buying entity identified on the ordering documents (i.e. Basic Order Agreement (BOA), Bid Buy Purchase Order, etc.) to confirm delivery date, time and location to ensure Warehouse/Receiving has staff on hand to receive equipment and that there isn't another delivery scheduled at the same time.
- 1.5.5. State agencies' normal hours are between 9:00 AM and 3:00 PM, Monday through Friday. Vendor must gain prior approval from the ordering entity to deliver after hours, or on weekends or State holidays.
- 1.5.6. If Vendor is unable, or anticipates that it will not be able, to fulfill an order in accordance with the requirements of the Contract, a credit equal to 5% of the cost of the item/items may be assessed.
- 1.5.7. Vendor will submit a request to delay order fulfillment to the ordering entity in writing within seventy-two (72) hours of receipt of the applicable order and will include in such request its best estimate of the duration of the delay and the reasons for the delay. At the ordering entity's discretion, the entity may choose to approve the delay, assess the penalty, and/or be relieved from its obligations to purchase any quantities of supplies or equipment in such order and may cancel such quantities effective upon notice to Vendor. The ordering entity may elect to pursue alternative sources to fulfill the obligations of the canceled order. Vendor shall, at its own cost, use commercially reasonable efforts to remedy any shortage of supply and resume meeting the requirements of the Contract as soon as possible.

## 1.6. SUBCONTRACTING

Subcontractors are allowed.

- 1.6.1. Will subcontractors be utilized?  Yes  No

A subcontractor is a person or entity that enters into a contractual agreement with a total value of \$100,000 or more with a person or entity who has a contract subject to the Illinois Procurement Code pursuant to which the person or entity provides some or all of the goods, services, real property, remuneration, or other monetary forms of consideration that are the subject of the primary State contract, including subleases from a lessee of a State contract.

All contracts with subcontractors where the annual value of the subcontract is greater than \$50,000 must include Standard Illinois Certifications completed by the subcontractor.

- 1.6.2. Please identify below subcontracts with an annual value of \$100,000 or more that will be utilized in the performance of the Contract, the names and addresses of the subcontractors, and a description of the work to be performed by each.

- Subcontractor Name: SDI Presence LLC

Amount to Be Paid: 5% of total contract value

Address: 200 E. Randolph St., Suite 3550, Chicago, IL 60601

Description of Work: SDI Presence, operating as a Business Enterprise Program (BEP) vendor, will collaborate with AHEAD on the seamless implementation of server and file system solutions to enhance the State’s digital infrastructure. The concerted efforts will center on reliability and efficiency of crucial components such as mainframe computers, applications, databases, mail systems, network architecture, and web services. SDI Presence’s expertise will not only encompass the deployment of Dell Server and File solutions but will also extent to optimizing operational performance to maximize efficiency. Through this strategic partnership, the objective is to modernize data management and accessibility for State operations and ensure the secure and efficient delivery of services to meet the diverse needs of the State.

- Subcontractor Name: Dell Marketing, L.P.
- Amount to Be Paid: Unknown at this time

Address: One Dell Way, Round Rock, Texas 78682

Description of Work: Dell is the manufacturer of the products. Dell additionally shall provide all Maintenance and Support Services for the products purchased under this Agreement. Dell may also provide certain Professional Services, which may be sku’ed or under a SOW if custom.

- 1.6.3. If the annual value of any the subcontracts is more than \$100,000, then the Vendor must provide to the State the Financial Disclosures and Conflicts of Interest for that subcontractor.
- 1.6.4. If at any time during the term of the Contract, Vendor adds or changes any subcontractors, Vendor is required to promptly notify, in writing, the State Purchasing Officer or the Chief Procurement Officer of the names and addresses and the expected amount of money that each new or replaced subcontractor will receive pursuant to this Contract. Any subcontracts entered into prior to award of this Contract are done at the sole risk of the Vendor and subcontractor(s).

**1.7. SUCCESSOR VENDOR**

Yes  No This Contract is for services subject to 30 ILCS 500/25-80. Heating and air conditioning service contracts, plumbing service contracts, and electrical service contracts are not subject to this requirement. Non-service contracts, construction contracts, qualification-based selection contracts, and professional and artistic services contracts are not subject

to this requirement.

If yes is checked, then the Vendor certifies:

- (i) that it shall offer to assume the collective bargaining obligations of the prior employer, including any existing collective bargaining agreement with the bargaining representative of any existing collective bargaining unit or units performing substantially similar work to the services covered by the Contract subject to its bid or offer; and
- (ii) that it shall offer employment to all employees currently employed in any existing bargaining unit who perform substantially similar work to the work that will be performed pursuant to this Contract.

**1.8. WHERE SERVICES ARE TO BE PERFORMED:** Unless otherwise disclosed in this section all services shall be performed in the United States. If the Vendor performs the services purchased hereunder in another country in violation of this provision, such action may be deemed by the State as a breach of the Contract by Vendor.

Vendor shall disclose the locations where the services required shall be performed and the known or anticipated value of the services to be performed at each location. If the Vendor received additional consideration in the evaluation based on work being performed in the United States, it shall be a breach of Contract if the Vendor shifts any such work outside the United States.

- Location where services will be performed: Chicago, IL; Oak Brook, IL; Libertyville, IL, or Remotely from other locations within the United States

Value of services performed at this location: 100% of services to be performed

## 2. PRICING

**2.1 FORMAT OF PRICING:** Vendor's pricing, provided in Section 2.5 of this Contract, shall be based on the terms and conditions set forth in Section 1 of this Contract and shall serve as the basis for the compensation terms of this Contract.

2.1.1 For all Dell Server and Storage products, line item prices must include all costs shipped F.O.B. Destination where physical delivery is applicable, and may not include any additional costs due to taxes (federal or otherwise) unless accompanied by proof the State is subject to the tax.

2.1.2 For all Dell Server and Storage services based on an hourly rate, such line item hourly-rate pricing must include all costs or otherwise, as expenses are not authorized within this Contract. Pricing for each labor position consists of two pricing methods as follows: (1) standard hourly rate which is based on no travel; and (2) travel hourly rate which shall only apply to roles requiring daily/ weekly travel and is inclusive of all travel expenses.

2.1.3 State governmental units and not-for-profit entities do not have any minimum order requirements.

2.1.4 Reserved.

**2.1.5 Economic Adjustment Clause (Services Only)**

2.1.5.1 The prices in this Contract must remain firm for the first year after the execution date of the Contract. Thereafter, one upward price adjustment may be applied no more frequently than once during any given one-year period. Such adjustment shall be based on the Consumer Price Index as posted by the U.S. Bureau of Labor Statistics.

2.1.5.1 All adjustment requests shall be made in writing. Vendor shall not be entitled to apply an upward price adjustment without first obtaining approval of such request from DoIT.

2.1.5.2 In the event a downward adjustment is warranted, the State reserves the right to adjust once during any given twelve (12) month period for this decrease. It will be the responsibility of Vendor to notify DoIT of any such decrease.

2.1.5.3 No further adjustments will be made once the maximum allowable adjustment has been calculated for the given one year period.

2.1.5.4 An economic adjustment which is not based on the CPI may be requested by Vendor or the State to the price of all Contract Line Items. The State may, in its sole discretion, accept an equitable adjustment in the Contract terms or pricing if pricing or availability of supply is affected by extreme and unforeseen volatility in the marketplace, that is, by circumstances that satisfy all the following criteria: (1) the volatility is due to causes wholly beyond Vendor's control, (2) the volatility affects the marketplace or industry, not just the particular Contract source of supply, (3) the effect on pricing or availability of supply is substantial, (4) the volatility so affects Vendor that continued performance of the Contract would result in a substantial loss, and (5) no price adjustment will be approved to compensate a vendor for inefficiency or for errors or omissions in judgment or for additional profit or overhead of any kind.

2.1.5.5 Requested adjustments shall include the contract number, item number, line number, bid price and requested price adjustment.

2.1.5.6 In all cases, Vendor must file a claim in writing for such adjustment prior to the services being performed or delivery of items. In any event, the claim for such adjustment will not apply to release orders provided prior to the date DoIT approved the economic adjustment request.

2.1.5.7 If Vendor has unresolved complaints filed against it for non-delivery of

or poor-quality service, its request may be denied until such time as all past complaints are resolved to the satisfaction of the State.

**2.1.6 Adjustment Clause for Manufacturer’s Suggested Retail Pricing (MSRP) Pricelist**

2.1.6.1 The prices in the submitted MSRP list must remain firm for the first year after the execution date of the Contract. Thereafter, a new MSRP pricelist may be submitted no more frequently than once during any given one-year period.

2.1.6.2 All MSRP pricelist requests shall be made in writing. Vendor shall not be entitled to apply an upward price adjustment without first obtaining approval of such request from DoIT.

2.1.6.3 In all cases, Vendor must file a claim in writing for such adjustment prior to the services being performed or delivery of items. In any event, the claim for such adjustment will not apply to release orders provided prior to the date DoIT approved the adjustment request.

2.1.6.4 If Vendor has unresolved complaints filed against it for non-delivery of or poor-quality service, its request may be denied until such time as all past complaints are resolved to the satisfaction of the State.

**2.2 TYPE OF PRICING:** The Illinois Office of the Comptroller requires the State to indicate whether the Contract price is firm or estimated at the time it is submitted for obligation. The total price of this Contract is estimated.

**2.3 EXPENSES ALLOWED:** Expenses are not allowed.

**2.4 DISCOUNT:** The State may receive a 0 % discount for payment within N/A days of receipt of correct invoice. This discount will not be a factor in making the award.

**2.5 VENDOR’S PRICING:**

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<b>Dell Certified Technical Analyst - Standard Hourly Rate</b> - Standard configuration, deployment, installation, upgrade and problem resolution for end-user desktop/laptop, printers, and network related hardware, operating systems, and software. Minimum 2-5 years of experience in functional area and specific product technology requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Technical Analyst - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Standard configuration, deployment, installation, upgrade and problem resolution for end-user desktop/laptop, printers, and network related hardware, operating systems and software. Minimum 2-5 years of experience in functional area and specific product technology requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified Sr. Technical Analyst - Standard Hourly Rate</b> - Moderately complex configuration, deployment, installation, upgrade and advanced problem resolution for end-user desktop/laptop, printers, network related hardware. Minimum 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified Sr. Technical Analyst - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Moderately complex configuration, deployment, installation, upgrade and advanced problem resolution for end-user desktop/laptop, printers, network related hardware. Minimum 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified Systems Administrator - Standard Hourly Rate</b> - Administration, tuning, complex configuration, installation, and problem resolution related to midrange server, mainframe, network, storage hardware, operating systems, systems software and technology products. Minimum 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Systems Administrator - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel.- Administration, tuning, complex configuration, installation, and problem resolution related to midrange server, mainframe, network, storage hardware, operating systems, systems software and technology products. Minimum 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified Systems Engineer - Standard Hourly Rate</b> - Build, configure, test, integrate and implement on-prem and cloud infrastructure systems and components, mid-range server, mainframe, storage, and network technology. Minimum 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified Systems Engineer - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel- Build, configure, test, integrate and implement on-prem and cloud infrastructure systems and components, mid-range server, mainframe, storage and network technology. Minimum 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified Systems Architect - Standard Hourly Rate</b> - Design, plan and implement technology solutions and components for on-prem and cloud infrastructure, mid-range server, mainframe, storage, and network technology. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Systems Architect - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel- Design, plan and implement technology solutions and components for on-prem and cloud infrastructure; mid-range server, mainframe, storage and network technology. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Infrastructure and Technical Ops (Integration, configuration and administration, deployment and support of systems hardware, operating systems and system software.)</p>	HR	■
<p><b>Dell Certified QA Analyst - Standard Hourly Rate</b> - Evaluate functionality, reliability, and performance of software applications, includes monitoring and development test plans, cases and scripts. Minimum 2-5 years of experience in functional area. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified QA Analyst - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel- Evaluate functionality, reliability and performance of software applications, includes monitoring and development test plans, cases and scripts. Minimum 2-5 years of experience in functional area. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Software Developer - Standard Hourly Rate</b> - Designs, codes, verifies, tests, documents, amends and refactors moderately complex applications, programs and scripts. Minimum 5-8 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Software Developer - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Designs, codes, verifies, tests, documents, amends and refactors moderately complex applications, programs and scripts. Minimum 5-8 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Sr. Software Developer - Standard Hourly Rate</b> - Plans, designs, codes, verifies, tests, documents, amends and refactors complex applications, programs and scripts. Minimum 8-12 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Sr. Software Developer - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Plans, designs, codes, verifies, tests, documents, amends and refactors complex applications, programs and scripts. Minimum 8-12 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Data Base Administrator - Standard Hourly Rate</b> - Administer, develop, configure, install, maintain standards, monitor performance, and investigate problems related to database tools and objects. Minimum 5-8 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Data Base Administrator - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. Administer, develop, configure, install, maintain standards, monitor performance, and investigate problems related to database tools and objects. Minimum 5-8 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Software Application Architect - Standard Hourly Rate</b> - Design, plan and implement software application solutions, components and modules, undertakes impact analysis and prototyping, leads recommendation of technologies, design, methods, tools and techniques. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Software Application Architect - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Design, plan and implement software application solutions, components and modules, undertakes impact analysis and prototyping, leads recommendation of technologies, design, methods, tools and techniques. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Software/Applications and Data (Software application development focuses on the design, analysis, development, testing of interface information and data.)</p>	HR	■
<p><b>Dell Certified Systems Administrator - Standard Hourly Rate</b> - Administration, complex configuration, tuning, installation, and problem resolution related to cloud service platforms, software, instances, modules and components. Minimum 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Systems Administrator - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. Administration, complex configuration, tuning, installation, and problem resolution related to cloud service platforms, software, instances, modules and components. Minimum 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■
<p><b>Dell Certified Systems Analyst - Standard Hourly Rate</b> - Evaluate, analyze, define, monitor, and configure enhancements to product and service modules and components to optimize process workflows, automation and performance. Minimum 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■
<p><b>Dell Certified Systems Analyst - Travel Hourly Rate</b> -The Travel Rate will only apply to roles requiring daily/ weekly travel. - Evaluate, analyze, define, monitor, and configure enhancements to product and service modules and components to optimize process workflows, automation and performance. Minimum 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■
<p><b>Dell Certified Software Engineer - Standard Hourly Rate</b> - Specifies, designs, codes, configures and delivers functionality for cloud service platforms, software, components and modules. Minimum 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■
<p><b>Dell Certified Software Engineer - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Specifies, designs, codes, configures and delivers functionality for cloud service platforms, software, components and modules. Minimum 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Software Architect - Standard Hourly Rate</b> - Design, plan, develop and implement architectures, components and complex solutions related to cloud service platforms and software. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■
<p><b>Dell Certified Software Architect - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Design, plan, develop and implement architectures, components and complex solutions related to cloud service platforms and software. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Cloud Services and Cyber (Platform, software, infrastructure and security as-a-service hosted or integrated hybrid solutions.)</p>	HR	■
<p><b>Dell Certified Business Analyst - Standard Hourly Rate</b> - Defines business requirements, manages scoping, coordinates activities with stakeholders to ensure priorities are accurately reflected. Minimum 5-8 years of experience in functional area. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Business Analyst - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Defines business requirements, manages scoping, coordinates activities with stakeholders to ensure priorities are accurately reflected. Minimum 5-8 years of experience in functional area. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Sr. Business Analyst - Standard Hourly Rate</b> - Defines business and systems requirements, manages scoping, coordinates activities with stakeholders to ensure priorities are accurately reflected. Minimum 5-8 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Sr. Business Analyst - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel- Defines business and systems requirements, manages scoping, coordinates activities with stakeholders to ensure priorities are accurately reflected. Minimum 5-8 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Project Coordinator - Standard Hourly Rate</b> - Executes and coordinates the delivery of tasks and activities related to a program, project or service, including communication, organizational change management, scheduling, and tracking of deliverables using appropriate methods and tools. Minimum 2-5 years of experience in functional area. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Project Coordinator - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Executes and coordinates the delivery of tasks and activities related to a program, project or service, including communication, organizational change management, scheduling, and tracking of deliverables using appropriate methods and tools. Minimum 2-5 years of experience in functional area. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Project Manager - Standard Hourly Rate</b> - Execution the successful completion of projects, adopting methods and tools to preparing plans, schedules, milestones, deliverables and dependencies. Coordinates activities with team and applies change control and risk management process. Minimum 5-8 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Project Manager - Travel Hourly Rate</b> -The Travel Rate will only apply to roles requiring daily/ weekly travel. - Execution the successful completion of projects, adopting methods and tools to preparing plans, schedules, milestones, deliverables and dependencies. Coordinates activities with team and applies change control and risk management process. Minimum 5-8 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Program Manager - Standard Hourly Rate</b> - Manages the execution of large, complex, high impact, and/or multiple project workstreams as part of an initiative. Leads planning using appropriate methods and tools for delivery. Minimum 8-12 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Program Manager - Travel Hourly Rate</b> - The Travel Rate will only apply to roles requiring daily/ weekly travel. - Manages the execution of large, complex, high impact, and/or multiple project workstreams as part of an initiative. Leads planning using appropriate methods and tools for delivery. Minimum 8-12 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■
<p><b>Dell Certified Enterprise Architecture - Standard Hourly Rate</b> - Design, plan, develop and implement complex enterprise architectures, components, and solutions related to cloud service platforms and software. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■

Dell Certified Labor Positions		
Description	Unit of Measure	Unit Price
<p><b>Dell Certified Enterprise Architecture - Travel Hourly Rate</b> -The Travel Rate will only apply to roles requiring daily/ weekly travel. - Design, plan, develop and implement complex enterprise architectures, components, and solutions related to cloud service platforms and software. Minimum 15 years in information technology industry with 5-8 years of experience in functional area and specific product technologies requested. Enterprise IT (Enterprise planning, organizational change management and transition across information technology functions.)</p>	HR	■

Dell Offerings and Maintenance and Support Services		
Description	Notes	Percent Off
Dell Brand Servers, Non-Cloud-Based	Dell Brand Servers Non-Cloud See Section 1.2.1 for details.	65.00%
Dell Branded Server and Storage Accessories	Dell Brand Server and Storage Accessories See Section 1.2.3 for details.	40.00%
Dell Branded Server and Storage Replacement and Upgrade Components	Dell Brand Server and Storage Replacement and Upgrade Components See Section 1.2.4 for details.	59.00%
Dell Branded Server and Storage- Cloud Solutions	Dell Brand Cloud Server and Storage Solutions See Section 1.2.7 for details.	56.00%
Dell Brand Storage, Non-Cloud-Based	Dell Brand Storage Non-Cloud See Section 1.2.2 for details.	55.00%
Education Credits	Dell Educational Discount: Dell Education Discount is a special program that offers discounts and exclusive deals for educational facilities. This program provides educational facilities with access to Dell server and storage products at a reduced price. With Dell Education Discount, educational facilities can save money on Dell server and storage products. This program is available to educational institution defined as a school (including a technical, trade, or vocational school), junior college, college or university that is: operated or directly supported by the United States; operated or directly supported by any State or local government or by a political subdivision of any State or local government; or approved by a State agency or subdivision of the State.	53.00%
Dell Hardware and Software Maintenance and Support Services	Dell Hardware and Software Maintenance and Support Services. See Section 1.2.6 for details.	55.00%

2.5.1. Renewal Compensation: N/A.

**2.6 MAXIMUM AMOUNT:** The total payments under this contract are not applicable as this is an indefinite quantity master contract.

### **3. TERM AND TERMINATION**

**3.1 TERM OF THIS CONTRACT:** This Contract shall be in effect beginning on the last date of execution through October 15, 2028.

3.1.1 In no event will the total term of the Contract, including the initial term, any renewal terms and any extensions, exceed ten (10) years. 30 ILCS 500/20-60

3.1.2 Vendor shall not commence billable work in furtherance of the Contract prior to final execution of the Contract except when permitted pursuant to 30 ILCS 500/20-80.

**3.2 RENEWAL:** N/A

**3.3 TERMINATION FOR CAUSE:** The State may terminate this Contract, in whole or in part, immediately upon notice to the Vendor if: (a) the State determines that the actions or inactions of the Vendor, its agents, employees or subcontractors have caused, or reasonably could cause, jeopardy to health, safety, or property, or (b) the Vendor has notified the State that it is unable or unwilling to perform the Contract.

If Vendor fails to perform to the State's satisfaction any material requirement of this Contract, is in violation of a material provision of this Contract, or the State determines that the Vendor lacks the financial resources to perform the Contract, the State shall provide written notice to the Vendor to cure the problem identified within the period of time specified in the State's written notice. If not cured by that date the State may either: (a) immediately terminate the Contract without additional written notice or (b) enforce the terms and conditions of the Contract.

For termination due to any of the causes contained in this Section, the State retains its rights to seek any available legal or equitable remedies and damages.

**3.4 TERMINATION FOR CONVENIENCE:** The State may, for its convenience and with thirty (30) days' prior written notice to Vendor, terminate this Contract in whole or in part and without payment of any penalty or incurring any further obligation to the Vendor.

Upon submission of invoices and proof of claim, the Vendor shall be entitled to compensation for supplies and services provided in compliance with this Contract up to and including the date of termination.

**3.5 OTHER TERMINATION:** The State may also terminate, in whole or in part, this Contract without advance notice pursuant to Section 3.7.

**3.6 SUSPENSION:** The State may also suspend, in whole or in part, this Contract without advance notice pursuant to Section 3.7.

**3.7 AVAILABILITY OF APPROPRIATION:** This Contract is contingent upon and subject to the availability of funds. The State, at its sole option, may terminate or suspend this Contract, in whole or in part, without penalty or further payment being required, if (1) the Illinois

General Assembly or the federal funding source fails to make an appropriation sufficient to pay such obligation, or if funds needed are insufficient for any reason (30 ILCS 500/20-60), (2) the Governor or the Agency reserves funds, or (3) the Agency determines, in its sole discretion or as directed by the Office of the Governor, that a reduction is necessary or advisable based upon actual or projected budgetary considerations or available funds for payment. Vendor will be notified in writing of the failure of appropriation or of a reduction or decrease and the Agency's election to terminate or suspend, in whole or in part, as soon as practicable. Any suspension or termination pursuant to this section will be effective upon the date of the written notice unless otherwise indicated.

#### **4. STANDARD BUSINESS TERMS AND CONDITIONS**

##### **4.1 PAYMENT TERMS AND CONDITIONS:**

- 4.1.1** Late Payment: Payments, including late payment charges, will be paid in accordance with the State Prompt Payment Act and rules when applicable. 30 ILCS 540; 74 Ill. Adm. Code 900. This shall be Vendor's sole remedy for late payments by the State. Payment terms contained in Vendor's invoices shall have no force or effect.
- 4.1.2** Minority Contractor Initiative: Any Vendor awarded a contract of \$1,000 or more under Section 20-10, 20-15, 20-25 or 20-30 of the Illinois Procurement Code (30 ILCS 500) is required to pay a fee of \$15. The Comptroller shall deduct the fee from the first check issued to the Vendor under the contract and deposit the fee in the Comptroller's Administrative Fund. 15 ILCS 405/23.9.
- 4.1.3** Expenses: The State will not pay for supplies provided or services rendered, including related expenses, incurred prior to the execution of this Contract by the Parties even if the effective date of the Contract is prior to execution.
- 4.1.4** Dell Refund Passthrough: In the event Dell provides a refund under a provision of the attached Dell Terms, Vendor shall provide a commensurate refund to the State.
- 4.1.5** Prevailing Wage: As a condition of receiving payment Vendor must (i) be in compliance with the Contract, (ii) pay its employees prevailing wages when required by law, (iii) pay its suppliers and subcontractors according to the terms of their respective contracts, and (iv) provide lien waivers to the State upon request. Examples of prevailing wage categories include public works, printing, janitorial, window washing, building and grounds services, site technician services, natural resource services, security guard and food services. The prevailing wages are revised by the Illinois Department of Labor and are available on the Illinois Department of Labor's official website, which shall be deemed proper notification of any rate changes under this subsection. Vendor is responsible for contacting the Illinois Department of Labor at 217-782-6206 or (<http://labor.illinois.gov>) to ensure understanding of prevailing wage requirements.
- 4.1.6** Federal Funding: This Contract may be partially or totally funded with Federal funds. If Federal funds are expected to be used, then the percentage of the good/service paid using Federal funds and the total Federal funds expected to be used will be provided to the awarded Vendor in the notice of intent to award.

**4.1.7 Invoicing:** By submitting an invoice, Vendor certifies that the supplies or services provided meet all requirements of this Contract, and the amount billed and expenses incurred are as allowed in this Contract. Invoices for supplies purchased, services performed, and expenses incurred through June 30 of any year must be submitted to the State no later than July 31 of that year; otherwise Vendor may have to seek payment through the Illinois Court of Claims. 30 ILCS 105/25. All invoices are subject to statutory offset. 30 ILCS 210.

4.1.7.1 Vendor shall not bill for any taxes unless accompanied by proof that the State is subject to the tax. If necessary, Vendor may request the applicable Agency’s Illinois tax exemption number and Federal tax exemption information.

4.1.7.2 Vendor shall invoice on a per order basis.

Send invoices to:

Agency:	See “Bill To” on approved order
Attn:	See “Bill To” on approved order
Address:	See “Bill To” on approved order
City, State Zip	See “Bill To” on approved order

For procurements conducted in BidBuy, the Agency may include in this Contract the BidBuy Purchase Order as it contains the Bill To address.

**4.2 ASSIGNMENT:** This Contract may not be assigned or transferred in whole or in part by Vendor without the prior written consent of the State.

**4.3 SUBCONTRACTING:** For purposes of this section, subcontractors are those with contracts with an annual value exceeding \$100,000 and who are specifically hired to perform all or part of the work covered by this Contract. Vendor must receive prior written approval before use of any subcontractors in the performance of this Contract. Vendor shall describe, in an attachment if not already provided, the names and addresses of all authorized subcontractors to be utilized by Vendor in the performance of this Contract, together with a description of the work to be performed by the subcontractor and the anticipated amount of money that each subcontractor is expected to receive pursuant to this Contract. If required, Vendor shall provide a copy of any subcontracts within fifteen (15) days after execution of this Contract. All subcontracts must include the same certifications that Vendor must make as a condition of this Contract. Vendor shall include in each subcontract the Standard Illinois Certification form available from the State. If at any time during the term of the Contract, Vendor adds or changes any subcontractors, then Vendor must promptly notify, by written amendment to the Contract, the State Purchasing Officer or the Chief Procurement Officer of the names and addresses, the expected amount of money that each new or replaced subcontractor will receive pursuant to the Contract, and the general type of work to be performed. 30 ILCS 500/20-120.

**4.4 AUDIT/RETENTION OF RECORDS:** Vendor and its subcontractors shall maintain books and records relating to the performance of this Contract and any subcontract necessary to support amounts charged to the State pursuant this Contract or subcontract. Books and

records, including information stored in databases or other computer systems, shall be maintained by the Vendor for a period of three (3) years from the later of the date of final payment under the Contract or completion of the Contract, and by the subcontractor for a period of three (3) years from the later of final payment under the term or completion of the subcontract. If Federal funds are used to pay Contract costs, the Vendor and its subcontractors must retain their respective records for five (5) years. Books and records required to be maintained under this section shall be available for review or audit by representatives of: the procuring Agency, the Auditor General, the Executive Inspector General, the Chief Procurement Officer, State of Illinois internal auditors or other governmental entities with monitoring authority, upon reasonable notice and during normal business hours. Vendor and its subcontractors shall cooperate fully with any such audit and with any investigation conducted by any of these entities. Failure to maintain books and records required by this section shall establish a presumption in favor of the State for the recovery of any funds paid by the State under this Contract or any subcontract for which adequate books and records are not available to support the purported disbursement. The Vendor or subcontractors shall not impose a charge for audit or examination of the Vendor's or subcontractor's books and records. 30 ILCS 500/20-65. Vendor and its subcontractors shall upon reasonable notice appear before and respond to requests for information from the Illinois Works Review Panel. 30 ILCS 559/20-25(d).

- 4.5 TIME IS OF THE ESSENCE:** Time is of the essence with respect to Vendor's performance of this Contract. Vendor shall continue to perform its obligations while any dispute concerning this Contract is being resolved unless otherwise directed by the State.
- 4.6 NO WAIVER OF RIGHTS:** Except as specifically waived in writing, failure by a Party to exercise or enforce a right does not waive that Party's right to exercise or enforce that or other rights in the future.
- 4.7 FORCE MAJEURE:** Failure by either Party to perform its duties and obligations will be excused by unforeseeable circumstances beyond its reasonable control and not due to its negligence, including acts of nature, acts of terrorism, riots, labor disputes, fire, flood, explosion, and governmental prohibition. The non-declaring Party may cancel this Contract without penalty if performance does not resume within thirty (30) days of the declaration.
- 4.8 CONFIDENTIAL INFORMATION:** Each Party to this Contract, including its agents and subcontractors, may have or gain access to confidential data or information owned or maintained by the other Party in the course of carrying out its responsibilities under this Contract. Vendor shall presume all information received from the State or to which it gains access pursuant to this Contract is confidential. Vendor information, unless clearly marked as confidential and exempt from disclosure under the Illinois Freedom of Information Act ("FOIA") (5 ILCS 140), shall be considered public. Unless otherwise agreed by the Parties, and then only upon receipt of the State's prior written consent, Vendor and its subcontractors shall not access or attain any personally identifiable information or sensitive information on or from the State's systems, and Vendor agrees that any such information is the confidential information of the State. In any event, Vendor shall implement and maintain reasonable security measures to protect any and all data, information, and records disclosed by the State under this Contract from unauthorized access, acquisition, destruction, use, modification, or disclosure. No confidential data collected, maintained, or used in the course of performance of this Contract shall be disseminated except as authorized by law and with the written consent of the disclosing

Party, either during the period of this Contract or thereafter. The receiving Party must return any and all data collected, maintained, created or used in the course of the performance of this Contract, in a non-proprietary, readily usable format, promptly at the end of this Contract, or earlier at the request of the disclosing Party, or notify the disclosing Party in writing of its destruction. The foregoing obligations shall not apply to confidential data or information lawfully in the receiving Party's possession prior to its acquisition from the disclosing Party; received in good faith from a third Party not subject to any confidentiality obligation to the disclosing Party; now is or later becomes publicly known through no breach of confidentiality obligation by the receiving Party; or that is independently developed by the receiving Party without the use or benefit of the disclosing Party's confidential information.

**4.9 USE AND OWNERSHIP:** Work for hire is generally not contemplated under this Contract. In the event that work for hire is required or requested by the State and becomes the subject of a contemplated purchase under this Contract, the Parties agree that related terms, such as provisions on intellectual property ownership, rights, and responsibilities, may be negotiated at that time and included in a written agreement signed by the Parties and attached to the relevant order relating to the work.

**4.10 INDEMNIFICATION AND LIABILITY:** Vendor shall indemnify and hold harmless the State, its agencies, officers, employees, agents and volunteers from any and all costs, demands, expenses, losses, claims, damages, liabilities, settlements and judgments, including in-house and contracted attorneys' fees and expenses related to third party claims: (a) any breach or violation by Vendor of any of its certifications, representations, warranties, covenants or agreements; (b) any actual or alleged death or injury to any person, damage to any real or personal property, or any other damage or loss claimed to result in whole or in part from Vendor's negligent performance; (c) any act, activity or omission of Vendor or any of its employees, representatives, subcontractors or agents; or (d) any actual or alleged claim that the products or services provided under this Contract infringe, misappropriate, or otherwise violate any intellectual property rights (including but not limited to patent, copyright, trade secret, or trademark rights) of a third party. Vendor shall also defend (subject to the consent of the Office of the Attorney General ("OAG")) the State against any and all third-party claims related to this Contract. In accordance with Article VIII, Section 1(a), (b) of the Constitution of the State of Illinois, the State may not indemnify private parties absent express statutory authority permitting the indemnification. The State shall not be liable for indirect, special, consequential, or punitive damages. In no event will either Party be liable for any indirect, special, punitive, incidental, or consequential damages, except as specifically provided in these State Terms, even if advised of the possibility of such loss or damage. Notwithstanding anything else contained in this Contract to the contrary, regardless of the form of action, but excluding Vendor's indemnification and defense obligations under this Section 4.10, Vendor's obligations under Sections 4.10.1 and 4.10.2, and any claims of death or injury to persons or real property, or claims of fraud or intentional misrepresentation resulting from the actions or inactions of Vendor, the total liability of Vendor to the State shall not exceed the greater of (i) three (3) times the total amount paid and payable to Vendor under this Contract or (ii) fifteen million dollars (\$15,000,000).

**4.10.1 DATA BREACH PREVENTION, NOTICE, AND REMEDIATION:** To the extent related to or in furtherance of the Vendor's performance under this Contract, Vendor shall ensure the security, storage, and integrity of the State's content, data, computers, networks, and systems (which may include the use of encryption technology to protect the State's content and data from unauthorized access). Notwithstanding anything to the contrary

in this Contract, to the extent that Vendor experiences or causes an information breach or security incident that impacts the State's data, content, computers, systems, or networks, Vendor shall immediately notify the State and will use best efforts to immediately remedy any such breach or incident, and to prevent any further breach or incident, at Vendor's expense, in accordance with applicable privacy rights, laws, regulations, policies, and standards, including but not limited to the Illinois Personal Information Protection Act (815 ILCS 530). Vendor shall reimburse the State for any and all costs incurred by the State in responding to, and mitigating damages caused by, any such breach or security incident, including all costs of notice and/or remediation.

**4.10.2 DATA LOSS AND DAMAGE TO STATE COMPUTER SYSTEMS:** Vendor shall adhere to all indemnification and liability obligations stated in this Contract and will remain liable where any damage or impairment to the State's computers, systems, and networks, or any loss or corruption of the State's data or content, is due to Vendor's negligent or intentional acts and omissions. Further, Vendor shall reimburse the State for any and all costs incurred by the State in restoring such data, content, computers, systems, or networks.

**4.11 INSURANCE:** Vendor shall, at all times during the term of this Contract and any renewals or extensions, maintain and provide a Certificate of Insurance naming the State as an additionally insured for all required bonds and insurance. Certificates may not be modified or canceled until at least thirty (30) days' notice has been provided to the State. Vendor shall provide: (a) General Commercial Liability insurance in the amount of \$1,000,000 per occurrence (Combined Single Limit Bodily Injury and Property Damage) and \$2,000,000 Annual Aggregate; (b) Auto Liability, including Hired Auto and Non-owned Auto (Combined Single Limit Bodily Injury and Property Damage), in amount of \$1,000,000 per occurrence; and (c) Worker's Compensation Insurance in the amount required by law. Insurance shall not limit Vendor's obligation to indemnify, defend, or settle any claims.

**4.12 INDEPENDENT CONTRACTOR:** Vendor shall act as an independent contractor and not an agent or employee of, or joint venturer with the State. All payments by the State shall be made on that basis.

**4.13 SOLICITATION AND EMPLOYMENT:** Vendor shall not employ any person employed by the State during the term of this Contract to perform any work under this Contract. Vendor shall give notice immediately to the Agency's director if Vendor solicits or intends to solicit State employees to perform any work under this Contract.

**4.14 COMPLIANCE WITH THE LAW:** The Vendor, its employees, agents, and subcontractors shall comply with all applicable Federal, State, and local laws, rules, ordinances, regulations, orders, Federal circulars and all license and permit requirements in the performance of this Contract. Vendor shall be in compliance with applicable tax requirements and shall be current in payment of such taxes. Vendor shall obtain at its own expense, all licenses and permissions necessary for the performance of this Contract.

**4.15 BACKGROUND CHECK:** Vendor affirms that it checks the criminal records of all applicants for felony convictions and misdemeanor convictions involving a violent act or threat of violence within five (5) years prior to employment, where permitted by law.

Whenever the State deems it reasonably necessary for security reasons, the State may conduct, at its expense, criminal and driver history background checks of Vendors and

subcontractors, officers, employees or agents performing services on State owned, leased or controlled property. Vendor or subcontractor shall reassign immediately any such individual who, in the reasonable opinion of the State, does not pass the background checks. The background checks shall be in compliance with all federal laws. The State further agrees as follows:

- Use of the information collected will be for the specific purpose of facilitating a background check;
- All information collected will be treated as confidential;
- The State will limit access to the information received and will properly store it in a reasonably secure manner;
- The State will promptly dispose in an appropriate manner all collected information when the purpose for which it was originally collected is no longer valid; and
- State must provide notice and consent forms. Vendor's and subcontractor's officers, employees or agents performing services on state owned, leased or controlled property not consenting shall be reassigned.

However, in no event can Vendor agree to waive the rights of its employees, nor can Vendor provide the State with any information protected by law, including but not limited to Vendor's background check data.

#### **4.16 APPLICABLE LAW:**

**4.16.1 PREVAILING LAW:** This Contract shall be construed in accordance with and is subject to the laws and rules of the State of Illinois.

**4.16.2 EQUAL OPPORTUNITY:** The Department of Human Rights' Equal Opportunity requirements are incorporated by reference. 44 Ill. Adm. Code 750.

**4.16.3 COURT OF CLAIMS; ARBITRATION; SOVEREIGN IMMUNITY:** Any claim against the State arising out of this Contract must be filed exclusively with the Illinois Court of Claims. 705 ILCS 505/1. The State shall not enter into binding arbitration to resolve any dispute arising out of this Contract. The State of Illinois does not waive sovereign immunity (including all rights provided in the State Lawsuit Immunity Act, 745 ILCS 5) by entering into this Contract.

**4.16.4 OFFICIAL TEXT:** The official text of the statutes cited herein is incorporated by reference. An unofficial version can be viewed at ([www.ilga.gov/legislation/ilcs/ilcs.asp](http://www.ilga.gov/legislation/ilcs/ilcs.asp)).

**4.17 ANTI-TRUST ASSIGNMENT:** If Vendor does not pursue any claim or cause of action it has arising under Federal or State antitrust laws relating to the subject matter of this Contract, then upon request of the Illinois Attorney General, Vendor shall assign to the State all of Vendor's rights, title and interest to the claim or cause of action.

**4.18 CONTRACTUAL AUTHORITY:** The Agency that signs this Contract on behalf of the State of Illinois shall be the only State entity responsible for performance and payment under this Contract. When the Chief Procurement Officer or authorized designee or State Purchasing Officer signs in addition to an Agency, he/she does so as approving officer and shall have no liability to Vendor. When the Chief Procurement Officer or authorized

designee or State Purchasing Officer signs a master contract on behalf of State agencies, only the Agency that places an order or orders with the Vendor shall have any liability to the Vendor for that order or orders.

- 4.19 EXPATRIATED ENTITIES:** Except in limited circumstances, no business or member of a unitary business group, as defined in the Illinois Income Tax Act, shall submit a bid for or enter into a contract with a State agency if that business or any member of the unitary business group is an expatriated entity.
- 4.20 NOTICES:** Notices and other communications provided for herein shall be given in writing via electronic mail whenever possible. If transmission via electronic mail is not possible, then notices and other communications shall be given in writing via registered or certified mail with return receipt requested, via receipted hand delivery or via courier (UPS, Federal Express or other similar and reliable carrier). Notices shall be sent to the individuals who signed this Contract using the contact information as provided with the signatures. Each such notice shall be deemed to have been provided at the time it is actually received. By giving notice, either Party may change its contact information.
- 4.21 MODIFICATIONS AND SURVIVAL:** Amendments, modifications and waivers must be in writing and signed by authorized representatives of the Parties. Any provision of this Contract officially declared void, unenforceable, or against public policy, shall be ignored and the remaining provisions shall be interpreted, as far as possible, to give effect to the Parties' intent. All provisions that by their nature would be expected to survive, shall survive termination. In the event of a conflict between the State's and the Vendor's terms, conditions and attachments, the State's terms, conditions and attachments shall prevail.
- 4.22 PERFORMANCE RECORD / SUSPENSION:** Upon request of the State, Vendor shall meet to discuss performance or provide contract performance updates to help ensure proper performance of this Contract. The State may consider Vendor's performance under this Contract and compliance with law and rule to determine whether to continue this Contract, suspend Vendor from doing future business with the State for a specified period of time, or whether Vendor can be considered responsible on specific future contract opportunities.
- 4.23 FREEDOM OF INFORMATION ACT:** This Contract and all related public records maintained by, provided to, or required to be provided to the State are subject to the Illinois Freedom of Information Act ("FOIA") notwithstanding any provision to the contrary that may be found in this Contract. 5 ILCS 140.
- 4.24 SCHEDULE OF WORK:** Any work performed on State premises shall be performed during the hours designated by the State and performed in a manner that does not interfere with the State and its personnel.
- 4.25 WARRANTIES FOR SUPPLIES AND SERVICES:**
- 4.25.1. Subject to Section 1.2.10 of this Contract, Dell warranties are as provided in the Dell Terms attachments to this Contract. Vendor shall ensure that all manufacturers' warranties are transferred to the State to the extent permitted by the manufacturer and shall provide to the State copies of such warranties upon request.
- 4.25.2. Vendor warrants that all services will be performed to meet the requirements of

this Contract in an efficient and effective manner by trained and competent personnel. Vendor shall monitor performances of each individual and shall immediately reassign any individual who does not perform in accordance with this Contract, who is disruptive or not respectful of others in the workplace, or who in any way violates the Contract or State policies.

4.25.3. EXCEPT AS SET FORTH IN THIS AGREEMENT, VENDOR MAKES NO OTHER WARRANTIES OF ANY KIND, WRITTEN OR ORAL, AND ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ARE HEREBY SPECIFICALLY DISCLAIMED.

**4.26 REPORTING, STATUS AND MONITORING SPECIFICATIONS:** Vendor shall immediately notify the State of any event that may have a material impact on Vendor's ability to perform this Contract.

**4.27 EMPLOYMENT TAX CREDIT:** Vendors who hire qualified veterans and certain ex-offenders may be eligible for tax credits. 35 ILCS 5/216, 5/217. Please contact the Illinois Department of Revenue (telephone #: 217-524-4772) for information about tax credits.

**4.28 SUPPLEMENTAL TERMS:** Notwithstanding any provision to the contrary in the Vendor's supplemental terms and conditions, or in any licensing agreement attached hereto:

**4.28.1** The procuring Agency and the State do not waive sovereign immunity (including all rights provided in the State Lawsuit Immunity Act, 745 ILCS 5);

**4.28.2** The procuring Agency and the State do not consent to be governed by the laws of any state other than Illinois;

**4.28.3** The procuring Agency and the State do not consent to be represented in any legal proceeding by any person or entity other than the Illinois Attorney General or his or her designee;

**4.28.4** The procuring Agency and the State shall not be bound by the terms and conditions contained in any click-wrap agreement, click-wrap license, click-through agreement, click-through license, end user license agreement or any other agreement or license contained or referenced in the software or any quote provided by Vendor, except as attached to this Contract.

**4.28.5** The procuring Agency and the State shall not indemnify Vendor or its subcontractors (including any equipment manufacturers or software companies);

**4.28.6** Vendor shall indemnify the procuring Agency and State pursuant to the terms and conditions of the Indemnification and Liability clause of this Contract;

**4.28.7** Vendor's liability shall be governed by the terms and conditions contained in the Indemnification and Liability clause of this Contract; and

**4.28.8** Vendor must ensure that all information technology, including electronic information, software, systems and equipment, developed or provided under this contract complies with the applicable requirements of the Illinois Information Technology Accessibility Act Standards as published at ([www.dhs.state.il.us/iitaa](http://www.dhs.state.il.us/iitaa)). 30 ILCS 587.

**4.29 SECURITY REQUIREMENTS:** The State of Illinois has specific security requirements for

information and systems. Vendor must ensure these requirements are fully understood and allocate sufficient project time and resources to address the security requirements.

An information security risk assessment, data classification and system categorization process and the submission of a system security plan must be completed and submitted to the Department of Innovation & Technology, Division of Information Security prior to the commencement of system development or solution delivery activities. Vendor must participate with the risk assessment and data classification and system categorization process. The formal risk assessment, data classification and system categorization process will be administered by the Illinois Department of Innovation & Technology, Division of Information Security. Vendor program and project management personnel must ensure the coordination of these activities with State of Illinois program and project management personnel.

If not specifically addressed in other Vendor Information Technology Requirements, Vendor must adhere to State of Illinois and Illinois Department of Innovation & Technology technology and security Policies, Procedures, and Standards. <https://www2.illinois.gov/sites/doi/support/policies/Pages/default.aspx>

Vendor must also adhere to a minimum security baseline as identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Systems and Organizations. <https://doi.org/10.6028/NIST.SP.800-53r>. If not specifically addressed in other Vendor Information Technology Requirements, Vendors must assure the adoption of, at minimum, the low security control baselines. Exceptions to this requirement must be approved by the Illinois Department of Innovation & Technology, Division of Information Security.

Cloud solutions must adhere to recommendations of the Cloud Security Alliance. Vendors may find guidance and cross-referencing to the NIST 800-53, Revision 5 with the Cloud Security Alliance controls at CSA (Cloudsecurityalliance.org).

State and Federal laws, rules and regulations as well as industry-specific guidelines require specific and often enhanced security controls on information and systems. The State of Illinois is required to comply with the below laws, standards and regulations. Vendors must ensure compliance with the below as appropriate based upon the formal risk assessment to include a data classification and system categorization process.

- Illinois Identity Protection Act (5 ILCS 179)
- Illinois Personal Information Protection Act (815 ILCS 530)
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Federal Bureau of Investigations Criminal Justice Information Services (CJIS) Security Policy, version 5.5, issued June 26, 2016
- Federal Centers for Medicare & Medicaid Services (CMS) MARS-E Document Suite, Version 2.0 Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges November 10, 2015.
- Federal Centers for Medicare & Medicaid Services Information Security



## 5. STATE SUPPLEMENTAL PROVISIONS

Agency Definitions

5.1.1 “Chief Procurement Officer” means the chief procurement officer appointed pursuant to 30 ILCS 500/10-20(a)(4).

5.1.2 “Governmental unit” means State of Illinois, any State agency as defined in Section 1-15.100 of the Illinois Procurement Code, officers of the State of Illinois, any public authority in Illinois which has the power to tax or any other public entity created by Illinois statute.

5.1.3 “Qualified not-for-profit agency” means any not-for-profit agency that qualifies under Section 45-35 of the Illinois Procurement Code and that either (1) acts pursuant to a board established by or controlled by a unit of local government or (2) receives grant funds from the State or from a unit of local government.

Required Federal Clauses, Certifications and Assurances

Public Works Requirements (construction and maintenance of a public work) 820 ILCS 130/4.

PREVAILING WAGE ACT: This Contract calls for the construction of a “public work”, within the meaning of the Illinois Prevailing Wage Act, 820 ILCS 130/.01 et seq. (“the Prevailing Wage Act”). The Prevailing Wage Act requires vendors and subcontractors to pay laborers, workers and mechanics performing services on public works projects no less than the current “prevailing rate of wages” (hourly cash wages plus amount for fringe benefits) in the county where the work is performed. The Code requires vendors that are awarded certain service contracts to pay service workers no less than the general prevailing wage rates of hourly wages (hourly cash wages plus amount for fringe benefits) in the county where the work is performed. The Illinois Department of Labor publishes the prevailing wage rates on its website at <http://labor.illinois.gov>. The Illinois Department of Labor revises the prevailing wage rates, and Vendor and any subcontractors have an obligation to check the Illinois Department of Labor’s website for revisions to prevailing wage rates. Please refer to the Illinois Department of Labor’s website. Vendor and any subcontractors rendering services under this Contract must comply with all requirements of the Prevailing Wage Act and Code, including but not limited to, all wage requirements and notice and record keeping duties.

Prevailing Wage (janitorial cleaning, window cleaning, building and grounds, site technician, natural resources, food services, security services, and printing, if valued at more than \$200 per month or \$2,000 per year) 30 ILCS 500/25-60.

PREVAILING WAGE ACT: This Contract is a service contract subject to the prevailing wage requirements of the Illinois Procurement Code, 30 ILCS 500/25-60 (the “Code”). The Prevailing Wage Act requires vendors and subcontractors to pay laborers, workers and mechanics performing services on public works projects no less than the current “prevailing rate of wages” (hourly cash wages plus amount for fringe benefits) in the

county where the work is performed. The Code requires vendors that are awarded certain service contracts to pay service workers no less than the general prevailing wage rates of hourly wages (hourly cash wages plus amount for fringe benefits) in the county where the work is performed. The Illinois Department of Labor publishes the prevailing wage rates on its website at <http://labor.illinois.gov>. The Illinois Department of Labor revises the prevailing wage rates, and Vendor and any subcontractors have an obligation to check the Illinois Department of Labor's website for revisions to prevailing wage rates. Please refer to the Illinois Department of Labor's website. Vendor and any subcontractors rendering services under this Contract must comply with all requirements of the Prevailing Wage Act and Code, including but not limited to, all wage requirements and notice and record keeping duties.

- EMPLOYMENT OF ILLINOIS WORKERS ON PUBLIC WORKS: In a period of excessive unemployment rates, State vendors (1) constructing or building any public works or (2) cleaning-up and disposing on-site of hazardous waste, and that clean-up or on-site disposal is funded or financed in whole or in part with State funds or funds administered by the State, are required to employ at least 90% Illinois laborers on such project. For projects involving clean-up and on-site disposal of hazardous waste, emergency response or immediate removal activities are excluded. This requirement applies to all labor whether skilled, semi-skilled or unskilled, whether manual or non-manual.

A period of excessive unemployment rates is defined as any month immediately following two consecutive calendar months during which the level of unemployment in the State of Illinois has exceeded 5% as measured by the United States Bureau of Labor Statistics in its monthly publication of employment and unemployment figures.

Any public works project financed in whole or in part by federal funds administered by the State of Illinois is covered under the provisions of this requirement, to the extent permitted by any applicable federal law or regulation. 30 ILCS 570.

Vendors may receive an exception from this requirement by submitting a request and supporting documents certifying that Illinois laborers are either not available or are incapable of performing the particular type of work involved. The certification must: (a) be submitted to the agency within the first quarter of the Contract term; (b) provide sufficient support that demonstrates the exception is met; (c) be signed by an authorized signatory of the vendor; and (d) be approved by the agency.

- ILLINOIS WORKS JOBS PROGRAM ACT (30 ILCS 559/20-1 et seq.): For a contract that utilizes appropriated capital funds in whole or in part, involves the construction of a public work, and has with an estimated total project cost of \$500,000 or more, Vendor must comply with the Illinois Works Apprenticeship Initiative (30 ILCS 559/20-20 to 20-25) and all applicable administrative rules. The "estimated total project cost" is a good faith approximation of the costs of the entire project. The goal of the Illinois Apprenticeship Initiative is that apprentices will perform either 10% of the total labor hours actually worked in each prevailing wage classification or 10% of the estimated labor hours in each prevailing wage classification, whichever is less. Vendor may seek from the Department of Commerce and Economic Opportunity ("DCEO") a waiver or reduction of this goal in certain circumstances pursuant to 30 ILCS 559/20-20(b). Vendor must ensure compliance

for the life of the entire project, including during the term of the Contract and after the term ends, if applicable, and will be required to report on and certify its compliance.

- Agency Specific Terms and Conditions  
Attachment A State of Illinois Security Requirements
- Other (describe)

- 5.1.1 The Chief Procurement Officer for General Services makes this Contract available to all governmental units and qualified not-for-profit agencies.
- 5.1.2 Vendor agrees to extend all terms and conditions, specifications, and pricing or discounts specified in this Contract for the items in this Contract to all governmental units and qualified not-for-profit agencies.
- 5.1.3 The supplies or services subject to this Contract shall be distributed or rendered directly to each governmental unit or qualified not-for-profit agency.
- 5.1.4 Vendor shall bill each governmental unit or qualified not-for-profit agency separately for its actual share of the costs of the supplies or services purchased.
- 5.1.5 The credit or liability of each governmental unit or qualified not-for-profit agency shall remain separate and distinct.
- 5.1.6 Disputes between vendors and governmental units or qualified not-for-profit agencies shall be resolved between the affected parties.
- 5.1.10 All terms and conditions in this Contract apply with full force and effect to all purchase orders.

Attachment A State of Illinois Security Requirements:

1. Vendor will notify the State of Illinois' Chief Information Security Officer within 24 hours of knowledge of any information breach or other security incident which impacts State of Illinois data. Email notification to: [DoIT.Security@illinois.gov](mailto:DoIT.Security@illinois.gov) and Subject Line should state "Breach Notification."
2. Vendor shall have a documented security incident policy and plan. Vendor must supply a copy at the request of the State of Illinois.
3. Vendor must comply with all United States Federal and State of Illinois laws, rules, and regulations.
4. Vendor must comply with all of the State of Illinois Enterprise Security Policies (<https://www2.illinois.gov/sites/doit/support/policies/Pages/default.aspx>).
5. Vendor must ensure that all information technology, including electronic information, software, systems and equipment, developed or provided under this contract complies with the applicable requirements of the Illinois Information Technology Accessibility Act Standards as published at ([www.dhs.state.il.us/iitaa](http://www.dhs.state.il.us/iitaa)). 30 ILCS 587. If available, Vendor must provide the State of Illinois their most recent Voluntary Product Accessibility Template (VPAT).
6. Vendor program and project management personnel must ensure coordination of activities with the State of Illinois governance program. Vendor must comply with all policies, standards, and procedures defined by the State of Illinois Department of Innovation and Technology's Enterprise Portfolio Management Office.
7. Vendor's system must interface with the State of Illinois' identity and access management solutions if authentication is required for access to the system.
8. Vendor's system must log activity within the system and have capacity to forward log information to the State of Illinois' security incident and event management system (SIEM). Vendor must meet the State of Illinois' Minimum Logging Requirements for the term of the Contract.
  1. *(See Security Appendix S1)*
9. Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State of Illinois with a System Operation Controls report (SOC 1) annually and applicable bridge/gap letter when vendor is hosting State of Illinois financial information.
10. Vendor certifies it can comply with at least one of the following requirements listed in order of preference.

10.1 Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State of Illinois with a System Operation Controls report (SOC 2 type 2) annually and applicable bridge/gap letter.

10.2 Vendor must provide the State of Illinois with a 3<sup>rd</sup> party risk assessment of the Vendor's system conducted within the last year including a 3<sup>rd</sup> party penetration test.

10.3 Vendor must provide the State of Illinois with a 3<sup>rd</sup> party risk assessment of the Vendor's system conducted within the last year.

10.4 Vendor must provide the State of Illinois with a 3<sup>rd</sup> party penetration test conducted within the last year.

10.5 Vendor must perform an internal security controls assessment to demonstrate compliance with the State of Illinois Vendor Security Controls, based on the current revision of NIST 800-53 security controls for a moderate system. *(See Security Appendix S2)*

11. Vendor must participate in an annual risk assessment and data classification and system categorization process. The formal risk assessment will be administered by the State of Illinois.

If Vendor cannot provide the SOC 1 and/or 2 report required above and any necessary bridge/gap letter or another appropriate third-party risk assessment as determined by the State of Illinois, then Vendor must perform an internal security controls assessment to demonstrate compliance with the State of Illinois Vendor Security Controls, based on the current revision of NIST 800-53 security controls for a moderate system. Vendor must provide attestation of compliance along with the results of this assessment documented in a Security Assessment Report (SAR) to the State of Illinois. This does not relieve the Vendor of the above requirement to submit a required SOC 1 and/or SOC 2.

1. *(See Security Appendix S2)*

12. Vendor must provide a Plan of Action and Milestones (POA&M) to the State of Illinois that addresses any control deficiencies identified during the State of Illinois' risk assessment, review of Vendor's SOC report(s), third-party assessment, and internal security controls assessment. The POA&M should describe the deficiencies in the security controls, address the residual risk, and detail plans for remediation. Vendor must provide the State of Illinois monthly updates regarding progress toward remediation of identified deficiencies.

1. *(See Security Appendix S3)*

13. Vendor must complete and provide the State of Illinois an Authority to Operate (ATO) or Authority to Connect (ATC) packet at the State of Illinois' request. This packet must be renewed annually.

14. Vendor must ensure all hosted data pertinent to this contract shall remain located within the contiguous United States.

15. Vendor must ensure encryption of State of Illinois data at rest and in motion. This encryption must comply with encryption security controls as defined in the most current version of the Federal Information Processing Standard (FIPS) 140 using Advanced Encryption Standard (AES) encryption with a minimum key length of 256 bits. Vendor must

provide proof of encryption. Vendor must provide the State of Illinois with the capabilities to manage encryption keys for data at rest.

16. Vendor must store data in a non-proprietary, readily accessible format, or Vendor must provide a solution, at no additional cost to the State of Illinois, to extract any State of Illinois data stored in Vendor's solution.

17. Vendor must only use State of Illinois data, for the purposes stated in this contract.

18. Vendor must maintain a robust and reliable data backup system. Vendor must supply a description of backup methodology, and this methodology must meet defined Maximum Tolerable Downtime (MTD) and Return to Operations (RPO) requirements.

19. Vendor must provide a written disaster recovery mythology and provide proof of annual disaster recovery testing, including issues discovered and remediation plans for the issues discovered.

20. Vendor may not use any State of Illinois data in any non-production system or in any other system outside the application/service procured under this contract.

21. Vendor must provide a copy of all State of Illinois data (in a non-proprietary format) to the State of Illinois without delay upon request by the State of Illinois.

22. Vendor must provide a copy of all State of Illinois data (in a non-proprietary format) to the State of Illinois prior to termination of contract.

23. Vendor must sanitize all media that contains or contained State of Illinois data. Vendor must use the more current revision of NIST Special Publication 800-88; Guidelines for Media Sanitization. Vendor must provide the State of Illinois with a written certification of media sanitization including the method, date and time.

24. Vendor must use a form of "crypto shredding" acceptable to the State of Illinois for rendering all State of Illinois data hosted by the Vendor inaccessible after a copy of all data has been provided to the State of Illinois.

25. Vendor and/or its agents must not resell nor otherwise redistribute information gained from its access to the State of Illinois data.

26. Vendor must not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the State of Illinois.

27. Vendor must allow the State of Illinois to perform vulnerability assessments.

1. *(See Security Appendix S5)*

28. Vendor must immediately remediate critical, high, and medium vulnerabilities within the application that are detected during the security assessments and are determined by the State of Illinois to pose an unacceptable risk.

29. Vendor must secure independent third-party penetration testing at regular intervals, in accordance with Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) recommendations. Vendor must supply the results of the testing to the State of Illinois upon request.

30. Vendor must supply a list of all non-proprietary/open source software used in their solution. Vendor must also include the version and Open Source Initiative (OSI) approved license type used for any open source software. If Open Source uses non-OSI approved licensing Vendor must include licensing terms and conditions.

**Security Appendix S1 – Minimum Logging Requirements**

- Input validation failures (e.g., protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g., database record set mismatch, invalid data encoding)
- Authentication successes and failures
- Authorization (access control) failures
- Session management failures (e.g., cookie session identification value modification)
- Application errors and system events (e.g., syntax and runtime errors, connectivity problems, performance issues, third-party service error messages, file system errors, file upload virus detection, configuration changes)
- Application and related systems start-ups and shut downs, and logging initialization (starting, stopping, or pausing)
- Use of higher-risk functionality (e.g., network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of systems administrative privileges, access by application administrators, all actions by users with administrative privileges, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads)
- Legal and other opt-ins (e.g., permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications)

**Security Appendix S2: Security Controls for Vendors**

Authoritative Document [NIST 800-53 v4 – Security and Privacy Controls](#)

**Access and Control (AC)**

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

**AC Security Controls and Control Enhancements** (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Access Control Policy and Procedures	AC-1	
• Account Management	AC-2	(1), (2), (3), (4)
• Access Enforcement	AC-3	
• Information Flow Enforcement	AC-4	
• Separation of Duties	AC-5	

• Least Privilege	AC-6	(1), (2), (5), (9), (10)
• Unsuccessful Logon Attempts	AC-7	
• System Use Notification	AC-8	
• Session Lock	AC-11	(1)
• Session Termination	AC-12	
• Permitted Actions without Identification or Authentication	AC-14	
• Remote Access	AC-17	(1), (2), (3), (4)
• Wireless Access	AC-18	(1)
• Access Control for Mobile Devices	AC-19	(5)
• Use of External Information Systems	AC-20	(1), (2)
• Information Sharing	AC-21	
• Publicly Accessible Content	AC-22	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Awareness and Training (AT)**

Organizations must (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

**AT - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Security Awareness and Training Policy and Procedures	AT-1	
• Security Awareness Training	AT-2	(2)
• Role-Based Security Training	AT-3	
• Security Training Records	AT-4	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Audit and Accountability (AU)**

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users, so they can be held accountable for their actions.

**AU - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Audit and Accountability Policy and Procedure	AU-1	
• Audit Events	AU-2	(3)
• Content of Audit Records	AU-3	(1)
• Audit Storage Capacity	AU-4	
• Response to Audit Processing Failures	AU-5	
• Audit Review, Analysis, and Reporting	AU-6	(1), (3)
• Audit Reduction and Report Generation	AU-7	(1)
• Time Stamps	AU-8	(1)
• Protection of Audit Information	AU-9	(4)
• Audit Record Retention	AU-11	
• Audit Generation	AU-12	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Certification, Accreditation, and Security Assessments (CA)**

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organization information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

**CA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Security Assessment and Authorization Policy and Procedures	CA-1	
• Security Assessments	CA-2	(1)
• System Interconnections	CA-3	(5)
• Plan of Action and Milestones	CA-5	

• Security Authorization	CA-6	
• Continuous Monitoring	CA-7	(1)
• Internal System Connections	CA-9	

Authority	
NIST	SP 800-53 Security and Privacy Controls
NIST	SP 800-53A Assessing Security Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Configuration Management (CM)**

Vendors must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

**CM - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Configuration Management Policy and Procedures	CM-1	
• Baseline Configuration	CM-2	(1), (3), (7)
• Configuration Change Control	CM-3	(2)
• Security Impact Analysis	CM-4	
• Access Restrictions for Change	CM-5	
• Configuration Settings	CM-6	
• Least Functionality	CM-7	(1), (2), (4)
• Information System Component Inventory	CM-8	(1), (3), (5)
• Configuration Management Plan	CM-9	
• Software Usage Restrictions	CM-10	
• User-Installed Software	CM-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Contingency Planning (CP)**

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

**CP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
<ul style="list-style-type: none"> <li>Contingency Planning Policy and Procedures</li> </ul>	CP-1	
<ul style="list-style-type: none"> <li>Contingency Plan</li> </ul>	CP-2	(1), (3), (8)
<ul style="list-style-type: none"> <li>Contingency Training</li> </ul>	CP-3	
<ul style="list-style-type: none"> <li>Contingency Plan Testing</li> </ul>	CP-4	(1)
<ul style="list-style-type: none"> <li>Alternate Storage Site</li> </ul>	CP-6	(1), (3)
<ul style="list-style-type: none"> <li>Alternate Processing Site</li> </ul>	CP-7	(1), (2), (3)
<ul style="list-style-type: none"> <li>Telecommunications Services</li> </ul>	CP-8	(1), (2)
<ul style="list-style-type: none"> <li>Information System Backup</li> </ul>	CP-9	(1)
<ul style="list-style-type: none"> <li>Information System Recovery and Reconstitution</li> </ul>	CP-10	(2)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Identification and Authentication (IA)**

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.

**IA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
<ul style="list-style-type: none"> <li>Identification and Authentication Policy and Procedures</li> </ul>	IA-1	
<ul style="list-style-type: none"> <li>Identification and Authentication (Organizational Users)</li> </ul>	IA-2	(1), (2), (3), (8), (11), (12)
<ul style="list-style-type: none"> <li>Device Identification and Authentication</li> </ul>	IA-3	
<ul style="list-style-type: none"> <li>Identifier Management</li> </ul>	IA-4	
<ul style="list-style-type: none"> <li>Authentication Management</li> </ul>	IA-5	(1), (2), (3), (11)
<ul style="list-style-type: none"> <li>Authenticator Feedback</li> </ul>	IA-6	
<ul style="list-style-type: none"> <li>Cryptographic Module Authentication</li> </ul>	IA-7	
<ul style="list-style-type: none"> <li>Identification and Authentication (Non-Organizational Users)</li> </ul>	IA-8	(1), (2), (3), (4)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Incident Response (IR)**

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

**IR - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Incident Response Policy and Procedures	IR-1	
• Incident Response Training	IR-2	
• Incident Response Testing	IR-3	(2)
• Incident Handling	IR-4	(1)
• Incident Monitoring	IR-5	
• Incident Reporting	IR-6	(1)
• Incident Response Assistance	IR-7	(1)
• Incident Response Plan	IR-8	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Maintenance (MA)**

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

**MA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
--------------------------	-----------	-----------------

• System Maintenance Policy and Procedures	MA-1	
• Controlled Maintenance	MA-2	
• Maintenance Tools	MA-3	(1), (2)
• Nonlocal Maintenance	MA-4	(2)
• Maintenance Personnel	MA-5	
• Timely Maintenance	MA-6	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Media Protection (MP)**

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

**MP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Media Protection Policy and Procedures	MP-1	
• Media Access	MP-2	
• Media Marking	MP-3	
• Media Storage	MP-4	
• Media Transport	MP-5	(4)
• Media Sanitization	MP-6	
• Media Use	MP-7	(1)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Physical and Environmental Protection (PE)**

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

**PE - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
<ul style="list-style-type: none"> <li>Physical and Environmental Protection Policy and Procedures</li> </ul>	PE-1	
<ul style="list-style-type: none"> <li>Physical Access Authorizations</li> </ul>	PE-2	
<ul style="list-style-type: none"> <li>Physical Access Control</li> </ul>	PE-3	
<ul style="list-style-type: none"> <li>Access Control for Transmission Medium</li> </ul>	PE-4	
<ul style="list-style-type: none"> <li>Access Control for Output Devices</li> </ul>	PE-5	
<ul style="list-style-type: none"> <li>Monitoring Physical Access</li> </ul>	PE-6	(1)
<ul style="list-style-type: none"> <li>Visitor Access Records</li> </ul>	PE-8	
<ul style="list-style-type: none"> <li>Power Equipment and Cabling</li> </ul>	PE-9	
<ul style="list-style-type: none"> <li>Emergency Shutoff</li> </ul>	PE-10	
<ul style="list-style-type: none"> <li>Emergency Power</li> </ul>	PE-11	
<ul style="list-style-type: none"> <li>Emergency Lighting</li> </ul>	PE-12	
<ul style="list-style-type: none"> <li>Fire Protection</li> </ul>	PE-13	(3)
<ul style="list-style-type: none"> <li>Temperature and Humidity Controls</li> </ul>	PE-14	
<ul style="list-style-type: none"> <li>Water Damage Protection</li> </ul>	PE-15	
<ul style="list-style-type: none"> <li>Delivery and Removal</li> </ul>	PE-16	
<ul style="list-style-type: none"> <li>Alternate Work Site</li> </ul>	PE-17	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Planning (PL)**

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

**PL - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
<ul style="list-style-type: none"> <li>Security Planning Policy and Procedures</li> </ul>	PL-1	
<ul style="list-style-type: none"> <li>System Security Plan</li> </ul>	PL-2	(3)
<ul style="list-style-type: none"> <li>Rules of Behavior</li> </ul>	PL-4	(1)
<ul style="list-style-type: none"> <li>Information Security Architecture</li> </ul>	PL-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls

IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Personnel Security (PS)**

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions, such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

**PS - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Personnel Security Policy and Procedures	PS-1	
• Position Risk Designation	PS-2	
• Personnel Screening	PS-3	
• Personnel Termination	PS-4	
• Personnel Transfer	PS-5	
• Access Agreements	PS-6	
• Third-Party Personnel Security	PS-7	
• Personnel Sanctions	PS-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Risk Assessment (RA)**

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

**RA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• Risk Assessment Policy and Procedures	RA-1	
• Security Categorization	RA-2	
• Risk Assessment	RA-3	
• Vulnerability Scanning	RA-5	(1), (2), (5)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**System and Services Acquisition (SA)**

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and or services outsourced from the organizations.

**SA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
<ul style="list-style-type: none"> <li>System and Services Acquisition Policy and Procedures</li> </ul>	SA-1	
<ul style="list-style-type: none"> <li>Allocation of Resources</li> </ul>	SA-2	
<ul style="list-style-type: none"> <li>System Development Life Cycle</li> </ul>	SA-3	
<ul style="list-style-type: none"> <li>Acquisition Process</li> </ul>	SA-4	(1), (2), (9), (10)
<ul style="list-style-type: none"> <li>Information System Documentation</li> </ul>	SA-5	
<ul style="list-style-type: none"> <li>Security Engineering Principles</li> </ul>	SA-8	
<ul style="list-style-type: none"> <li>External Information System Services</li> </ul>	SA-9	(2)
<ul style="list-style-type: none"> <li>Developer Configuration Management</li> </ul>	SA-10	
<ul style="list-style-type: none"> <li>Developer Security Testing and Evaluation</li> </ul>	SA-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**System and Communications Protection (SC)**

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries for the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

**SC - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
--------------------------	-----------	-----------------

• System and Communication Protection Policy and Procedures	SC-1	
• Application Partitioning	SC-2	
• Information in Shared Resources	SC-4	
• Denial of Service Protection	SC-5	
• Boundary Protection	SC-7	(3), (4), (5), (7)
• Transmission Confidentiality and Integrity	SC-8	(1)
• Network Disconnect	SC-10	
• Cryptographic Key Establishment and Management	SC-12	
• Cryptographic Protection	SC-13	
• Collaborative Computing Devices	SC-15	
• Public Key Infrastructure Certificates	SC-17	
• Mobile Code	SC-18	
• Voice Over Internet Protocol	SC-19	
• Secure Name/Address Resolution Service (Authoritative Source)	SC-20	
• Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21	
• Architecture and Provisioning for Name/Address Resolution Service	SC-22	
• Session Authenticity	SC-23	
• Protection of Information at Rest	SC-28	
• Process Isolation	SC-39	
Authority		
CFR	HIPAA 45 CFR - 160, 162, 164	
NIST	SP 800-53 Security and Privacy Controls	
FIPS	200 Minimum Security Controls	
IRS	1075 Tax Information Security Guidelines	
DoIT	DoIT Policies and Associated Standards and Guidelines	

**System and Information Integrity (SI)**

Organizations must: (i) identify, report, and correct information and information systems flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems, and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

**SI - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):**

Security Control Summary	Control #	Enhancement #'s
• System and Information Integrity Policy and Procedures	SI-1	
• Flaw Remediation	SI-2	(2)
• Malicious Code Protection	SI-3	(1), (2)
• Information System Monitoring	SI-4	(2), (4), (5)
• Security Alerts, Advisories and Directives	SI-5	
• Software, Firmware, and Information Integrity	SI-7	(1), (7)

• Spam Protection	SI-8	(1), (2)
• Information Input Validation	SI-10	
• Error Handling	SI-11	
• Information Handling and Retention	SI-12	
• Memory Protection	SI-16	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
DoIT	DoIT Policies and Associated Standards and Guidelines

**Security Appendix S3 - Plan of Actions and Milestones Template**

Identified Deficiency	Residual Risk	Detailed Remediation Plan with Timeline	Expected Completion Date

**Security Appendix S5 – Vulnerability Assessment**

- Vendor shall request on behalf of the State of Illinois to perform vulnerability assessments on the cloud-hosting vendor’s website(s); provided, however, that in lieu of

such vulnerability assessments, the State of Illinois shall accept confirmation of a successful penetration testing in the last twelve months.

- If the Parties agree that the vulnerability assessment is necessary for Vendor, Vendor shall be permitted to supervise such assessment and Vendor must execute the State of Illinois Vulnerability Scanning Agreement prior to the vulnerability assessment. In the event the State of Illinois requests the vulnerability assessment from Dell or other relevant third parties, Vendor shall reasonably assist in such a request,  
*(See DoIT Scanning Agreement)*

- Under the circumstances described above, State of Illinois may, with reasonable notice to Vendor, conduct a security assessment of Vendor's solution, which may include the following:

- Prior to initial "official" production role out of the application,
  - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application
  - Manual verification of scan results with the same credentials
  - Manual testing of the application for vulnerabilities
  - State of Illinois will not conduct any Denial of Service (DOS) attacks
  - State of Illinois will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)
- On a quarterly basis for the for the first year after initial production deployment,
  - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application
  - Manual verification of scan results with the same credentials
  - Manual testing of the application for vulnerabilities
  - State of Illinois will not conduct any DOS attacks
  - State of Illinois will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)
- Prior to any enhancements or upgrades being deployed to production after the initial "official" production role out of the application,
  - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application
  - Manual verification of scan results with the same credentials
  - Manual testing of the application for vulnerabilities
  - State of Illinois will not conduct any DOS attacks
  - State of Illinois will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

- Monthly vulnerability scan – no whitelisting, non-credentialed scan (same day every month)

### **DoIT Scanning Agreement**

## Agreement

This agreement is between Department of Innovation & Technology \ Offensive Security Unit (hereinafter referred to as the "risk assessor") and Penetration Testing Services client (hereinafter referred to as the "client") for the supply of Penetration Testing services by the risk assessor for the client.

Whereas the risk assessor provides certain computer and systems security consulting and testing services including Penetration Testing services; and

Whereas the client wishes to retain the risk assessor to provide computer and systems security services, specifically Penetration Testing services; therefore

The client does hereby retain the risk assessor for the purpose of providing Penetration Testing services on the client's computers and/or systems.

The risk assessor will notify the client's project leader of the approximate times that the penetration tests will take place.

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the client the opportunity to address the identified issues in a planned manner, thus providing them the opportunity to significantly raise the level of their security protection. The client understands that Internet security is a continually growing and changing field and that testing by Department of Innovation & Technology \ Offensive Security Unit does not mean that the client's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and frequently do come from internal sources whose access is not a function of system configuration and/or external access security issues.

The client has provided the risk assessor with certain required information regarding the scope and range of the tests and the client hereby warrants that all information provided is true and accurate and that the client owns or is authorized to represent the owners of the computers and systems described. The client further warrants and represents that he/she is authorized to enter into binding legal agreements. The services provided by the risk assessor are provided in reliance on the above warrants.

The risk assessor shall be under no liability whatsoever to the client for any indirect loss and/or expense (including loss of profit) suffered by the client arising out of any actual or possible breach, by the risk assessor, of this agreement. In the event of any breach of this agreement by the risk assessor the remedies of the client shall be limited to a maximum of the fees paid by the client, for this engagement.

Both parties shall maintain this agreement as confidential. Unless required by law, no information about this agreement (including the agreement terms and fees) shall be released by either party. Information about the client's business, computer systems or security situation that the risk assessor obtains during the course of the work will not be released to any third party without prior written approval unless required by law.

The risk assessor and the client have imparted and may from time to time impart to each other certain confidential information relating to each other's business including specific documentation. Each party agrees that it shall use such confidential information solely for the purposes of the service and that it shall not disclose directly or indirectly to any third party such information. Where disclosure to a third party is required, prior notice of such disclosure will be made. The third party to which such disclosure will be made, will be required to agree to a duly binding agreement to maintain in confidence the information to be disclosed to the same extent at least as the parties are bound. To the extent that disclosure is requested by the Auditor General or otherwise authorized auditor, no additional agreement will be required.

Upon completion of the Penetration Testing service, the reports (deliverables) will be encrypted and delivered to the client while all other data related to the service will be securely stored, destroyed, or returned to the client (at client's option).

This agreement is subject to the laws of the State of Illinois, USA. All disputes arising out of this agreement shall be subject to the exclusive jurisdiction of the State of Illinois, USA.

Neither party shall be liable for any default due to any act of God, war, strike, lockout, industrial action, fire, flood, drought, storm or other event beyond the reasonable control of either party.

Signature \_\_\_\_\_ Date \_\_\_\_\_  
Authorized Client

Signature \_\_\_\_\_ Date \_\_\_\_\_  
Authorized Risk Assessor

## Dell Commercial Terms of Sale

These Commercial Terms of Sale ("CTS") are entered into by Supplier(s) (as defined below) and the State of Illinois, through the Department of Innovation and Technology (the "State" or "Customer"), and apply to orders for hardware, software, and services that are placed through reseller Ahead, Inc. ("Reseller") under State Contract #CMT4040325 (the "Contract") between the State and Reseller ("Orders"). Dell will perform Services and provide Products (as defined below) to the State through the Reseller according to this CTS and the other documents listed below, which are executed together with and included herein as exhibits to the CTS (collectively, the "Dell Terms"):

- 1) this CTS,
- 2) Exhibit A: the Dell Software End User License Agreement ("EULA"),
- 3) Exhibit B: the Dell Cloud Service Offerings Agreement ("CSOA"),
- 4) Exhibit C: the Dell Cloud Services Data Processing Addendum ("DPA"),
- 5) Exhibit D: the Dell APEX Subscriptions Terms for Partner End Users-US Public ("APEX-Subscriptions"), and
- 6) Exhibit E: the Dell Privacy Statement—United States ("Privacy Statement"), posted at: <https://www.dell.com/learn/us/en/uscorp1/policies-privacy> (which shall not impose any legal obligations on the State).

In the event of any ambiguity, inconsistency, or conflict, the following order of precedence will apply: (i) this CTS; (ii) the EULA; (iii) the CSOA and/or the APEX-Subscriptions, (iv) the DPA; and (v) any additional document referenced by hyperlink or otherwise within this CTS or the other Dell Terms (regardless of any language stating that the additional document is incorporated in the referencing document), including but not limited to the Privacy Statement and any Offering Specific Terms (as defined in Section 1.3 below).

For the avoidance of doubt, the parties agree that regardless of and to the exclusion of any language to the contrary contained in any other documents, including the Dell Terms and any other documents referenced or linked therein, the State cannot indemnify Supplier(s) or any other private parties, does not consent to be governed by the laws of any state other than Illinois, does not waive any rights under the State Lawsuit Immunity Act (745 ILCS 5), and does not consent to authorize any costs or fees beyond those specifically authorized in an Order it has placed under the Contract. All payment terms are between the State and Reseller, as set forth and controlled by the State Prompt Payment Act (30 ILCS 540). Any possible refund options provided for in the Dell Terms will be extended to the State by Reseller under the Contract.

The term "Supplier(s)" means, as applicable:

EMC Corporation ("EMC")  
176 South Street  
Hopkinton, Massachusetts 01748

and

Dell Marketing L.P. ("Dell")  
One Dell Way  
Round Rock, Texas 78682  
Legal Notices:  
[Dell\\_Legal\\_Notices@Dell.com](mailto:Dell_Legal_Notices@Dell.com)

The State and Supplier(s) are each a party and together the parties to this CTS. Orders may also be placed under the Contract by all governmental units and qualified not-for-profit agencies within the State of Illinois, for which all of the Dell Terms (as listed above) will also apply.

## 1. Subject Matter and Parts of CTS.

**1.1 Scope.** This CTS governs Supplier's provisioning of Products Services and Third Party Products (if applicable) (collectively "Offerings") in connection with Orders placed through Reseller under the Contract, for Customer's own internal use (which includes all State of Illinois governmental purposes).

**1.2 Products and Services.** "Products" are either: (i) Supplier-branded IT hardware products ("Equipment") or (ii) Supplier-branded generally available software, whether microcode, firmware, operating systems or applications ("Software").

Software includes "Subscription Software" licensed by Supplier as a stand-alone product on a subscription basis.

"Services" are defined as: (a) Supplier's standard service offerings for maintenance and support of Products or Subscriptions ("Support Services") and (b) consulting, deployment, implementation and any other services that are not Support Services ("Professional Services").

"Subscriptions" means Supplier-branded offerings provided to Customer for a defined time period ("Subscription Term") and priced based on the Subscription Term or other applicable metrics, and consisting of: (a) cloud offerings; or (b) Products or Services offered as a subscription, on an "as-a-service" basis or on a flexible consumption basis. Subscriptions do not include Subscription Software.

"Third Party Products" means hardware, software, products, subscriptions, or services that are not "Dell" or "Dell EMC" branded. Products exclude Services and Third Party Products.

**1.3 Framework.** This CTS contains the terms and conditions applicable to all Offerings, as may be supplemented by specific terms for certain Offerings available at [www.dell.com/offeringspecificterms](http://www.dell.com/offeringspecificterms), in a Service Specification, a Service Description, a Services Offering Description, a Product Notice, a Subscription Specification or in a "Schedule" to these Terms of Sale (collectively "Offering Specific Terms"), which are all considered part of these Terms of Sale by reference. The version of the applicable document that is effective as of the date of the applicable Order, shall be deemed applicable to the Order.

**1.4 Affiliates.** To fulfill Orders under this CTS, Supplier may utilize Dell Inc. or Dell Inc.'s subsidiaries, where "Subsidiaries" includes any other entity that Supplier directly or indirectly controls, is owned by, controlled by or under common ownership, and with respect to Dell Inc., its wholly owned or wholly controlled subsidiaries, where "Control" means more than 50% of the voting power or ownership interests ("Affiliate" or "Affiliates").

## 2. Quoting and Ordering.

**2.1 Reserved.**

**2.2 Orders Submitted Through Reseller.** Any purchase under the Contract will be made by submitting an order through Reseller. All invoicing, payment, returns, ordering, pricing and cancellation terms for the purchase will be as agreed in the Contract.

**2.3 Reserved.**

**2.4 Service-Specific Terms.** Scope and details of customized Professional Services not covered by Offering Specific Terms or as otherwise required in the Contract or these Dell Terms shall be documented in a mutually agreed Statement of Work between the State and Reseller ("SOW").

## 2.5 **Reserved.**

**2.6 Revision of Components.** Supplier may revise the components in a Product as long as the Product still substantially meets or exceeds the specifications as per the documentation of the ordered Product.

## 3. **Reserved.**

## 4. **Software Licenses.**

Customer's rights to use the Software delivered by Supplier are governed by the terms of the EULA. Unless expressly otherwise agreed, microcode, firmware or operating system software required to enable the Equipment with which it is shipped to perform its basic or enhanced functions, is licensed for use solely on such Equipment.

## 5. **Services.**

Supplier shall provide all Support Services. Depending on the type of Professional Services that may be at issue in a given Order, Reseller or Supplier (or a combination of the two) will provide Professional Services. Reseller and/or Supplier will provide such Professional Services (including any Deliverables) in accordance with the applicable Service Description, Reseller SOW, or other agreed upon documentation for such Services ("Service Specification") for the period agreed in the Order.

Supplier will provide Subscriptions in accordance with the Services Offering Description, Supplier's standard documentation for the Subscription or other agreed upon documentation for such Subscription ("Subscription Specification").

The Subscription activation process and the Subscription Term are described in the Subscription Specification and the Order entered into between the State and Reseller.

### 5.1 **Support Services.**

**A. Scope and Term.** Supplier shall provide Support Services in accordance with the applicable Service Description or Product Notice, for the (initial or renewal) period agreed in the applicable Order. Unless otherwise agreed by the parties in a writing included with an Order, the initial Support Services procured together with the purchase of a Product start on the commencement date of the applicable warranty period (as specified in clause 7). Pro Support technical support will be included for all Equipment ordered and run for a period of three (3) years, unless the State chooses to purchase a higher level or longer-term period of support.

**B. Support Availability and Release Cycles.** Availability of Support Services is governed by Supplier's "End-of-Service-Life" policies, available at [www.dell.com/support](http://www.dell.com/support) or as made available to Customer upon request ("Support Policies"). No sooner than 180 days, Supplier shall provide Customer written notice of any change to an applicable End of Sales Support for applicable Equipment(s) that may result in a reduction in the availability of previously ordered Support Services. End-of-Service-Life notices will follow End of Sales Support notices and may vary based on product types and availability of supplies. It shall be Customer's sole responsibility to provide Supplier with current email address to receive Support Availability notices. Customer's sole and exclusive remedy for such termination will be the credit by Reseller of any pre-paid fees for Support Services that will not be provided as a result of such termination. Unless stated otherwise in the applicable Support Policies, Support Services for Software apply only to the current and the immediately prior release of the Software.

**C. Limitations.** Support Services do not cover any of the following: (i) problems that are excluded from warranty coverage according to clause 7.4, below; (ii) problems that cannot be reproduced at Supplier's facility or via remote access to Customer's facility; (iii) onsite activities for Equipment that is located outside of the applicable service area (unless otherwise provided in a Service Description); (iv) providing media replacement, operating supplies, cosmetic accessories or parts such as frames, and cover or support on those items; or (v) repairing damage or defects in Equipment that are purely cosmetic and do not affect device functionality.

**D. Maintenance Tools and Spare Parts.** Supplier may, at its discretion, store tools and spare parts used by Supplier to perform diagnostic or remedial activities in connection with Products at the Customer's site or on Customer's systems, subject to State security policies and procedures in the State's discretion as provided to the Supplier in writing in advance, and Customer agrees that such are for use only by Supplier authorized personnel and further authorizes Supplier to remove and/or disable them when no longer needed by Supplier to provide its Services.

**E. Replacements.** All replaced Equipment or components thereof shall be returned to Supplier and become the property of Supplier upon receipt of the replaced Equipment or components at the specified Supplier facility unless specifically agreed otherwise by State and Supplier.

Customer shall return a replaced component or Equipment within 30 business days after receipt of Supplier's written request giving notice. To the extent any issues arise under this provision, the parties will work together in good faith to find a solution. Any additional costs or fees will require prior internal State approvals, and are subject to and governed by applicable laws and administrative rules, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCs 5/33E-9). If Supplier determines that a component of a defective Equipment product is "customer-replaceable", i.e. one that is easily disconnected and reconnected, or if the Supplier determines that the Equipment should be replaced as a whole, Supplier reserves the right to send Customer a component or whole replacement Equipment for exchange.

**F. Data Responsibility.** Supplier shall not access or use any Customer production data stored on the Products, unless Customer has expressly authorized Supplier to do so. Unless a data deletion service is expressly ordered from Supplier, Customer is responsible for removing all information and data stored on replaced parts, or on any other items or Product before it is returned to Supplier.

**G. Customer-Initiated Changes.** If the Product is covered by Support Services and Customer intends: (i) to relocate Equipment to a different installation site (where applicable to the Product); (ii) to change the hardware configuration on its own; or (iii) to deny the activation or to disable remote support features of a Product, Customer shall notify Supplier in advance.

Supplier shall notify Customer in the event that it believes that a Customer-initiated change may limit Supplier's ability to provide Support Services, increases Supplier's costs, or otherwise causes adverse effects. Proactive support capabilities, response times, or other service levels may temporarily be unavailable. The parties will work together in good faith to address and resolve any such issues. Any additional fees will require prior internal State approvals and are subject to and governed by applicable laws and administrative rules, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

## **5.2 Grant of License Rights in Deliverables.**

**A.** "Deliverables" means any reports, analyses, scripts, code, or other work results that Supplier delivers to Customer within the framework of fulfilling obligations under a Service Specification or SOW in connection

with any Services.

**B. "Proprietary Rights"** mean all patents, copyrights, trademarks, trade secrets, or other intellectual property rights of a party.

**C.** Subject to Customer's compliance with Supplier's Proprietary Rights incorporated into any Deliverables, and Customer's material compliance with the terms of this CTS, the Dell Terms, and the applicable Service Specification (but expressly excluding all issues related to the timing of payments, which shall not be considered a material breach), Supplier grants Customer a non-exclusive, non-transferable, revocable (in case of any breach of this CTS or any applicable Service Specification or SOW) non-sublicensable license to use the Deliverables for Customer's internal business operations (which include all State of Illinois governmental purposes). Customer may authorize its service providers to use the Deliverables, but solely on Customer's behalf, and solely for State of Illinois governmental purposes. To the extent any additional or different terms may be needed to address the rights of the Parties with respect to specific Deliverables contemplated for a particular Order, the Parties may negotiate and provide such applicable terms in a writing executed and attached to the Order at issue.

**D.** Each party reserves for itself all Proprietary Rights that it has not expressly granted to the other herein. The license granted in this clause 5.2. does not apply to: (i) Customer-furnished materials; (ii) any Products; (ii) Subscriptions, or (iii) items licensed or otherwise provided under a separate agreement. Supplier is not limited in developing, using, or marketing services or products that are similar to the Deliverables or Professional Services provided hereunder, any Service Specification, or, subject to Supplier's confidentiality obligations to Customer, in using the Deliverables or performing similar Professional Services for any other projects. Supplier(s) will not reproduce or otherwise incorporate State's Confidential Information into any Deliverables or Professional Services that are provided to other Supplier customers.

**E. Customer Furnished Materials.** Customer retains its Proprietary Rights in materials it furnishes to Supplier for use in connection with the performance of Professional Services. Customer grants Supplier a non-exclusive, non-transferable right, under Customer's Proprietary Rights, to use the Customer-provided materials solely for the benefit of Customer in fulfilling Supplier's obligations under this CTS.

**F. Reserved.**

**5.3 Customer Responsibilities.** In connection with Services, at no charge to Supplier, Customer shall: (i) provide Supplier personnel with timely access to appropriate facilities, space, power, documentation, files, data, information, additional software (if needed), all subject to State security policies and procedures as provided to the Supplier in writing and in the State's reasonable discretion; (ii) use skilled and authorized Customer personnel to assist and cooperate with Supplier in the provision of the Services as reasonably requested by Supplier; (iii) be responsible for physical and network security and all conditions in its business necessary for due performance of Services; (iv) allow Supplier remote and onsite access to the Products and Customer's infrastructure environment, as required, scheduled in advance (except as otherwise may be agreed by the parties as needed) subject to State's written security policies and procedures provided to Supplier and in the State's reasonable discretion; and (v) where applicable, notify Supplier in a reasonable amount of time when Products fail and provide Supplier with sufficient details of the failure such that the failure can be reproduced by Supplier. For Professional Services, details may be set forth in the Service Specification.

**5.4 Termination of Services.** A termination for convenience of Services shall only be permitted in accordance with the terms of the Contract. Either party may terminate Services for material breach by the other party (excluding all issues relating to the timing of payments, which shall not be considered a material breach) if such other party has failed to cure such breach within a reasonable grace period of no less than

30 days as set forth by the other party in writing.

**6 Reserved.**

**7 Warranty.**

**7.1 Product Warranty.**

**A. Equipment Warranty.** The Warranty period for Equipment will be 3 years, unless the State chooses to purchase a higher level of warranty or extended warranty option (or otherwise extend an existing warranty). Pro Support technical support will be included for all Equipment ordered and apply for the same period, unless the State chooses to purchase a higher level or longer-term period of support. Supplier warrants that Equipment, under normal usage and with regular recommended service, will be free from material defects in material and workmanship, and that Equipment will perform substantially in accordance with the corresponding standard documentation issued by Supplier for the applicable Equipment. Unless provided otherwise in a Schedule, additional terms governing the limited warranties for Equipment are found at [www.dell.com/warrantyterms](http://www.dell.com/warrantyterms) or in the applicable documentation or Product Notice for the specific Equipment. Supplier's entire liability for a breach of this warranty shall be for Supplier, at its option and cost, to repair or to replace the affected Equipment, and, if Supplier is unable to effect such within a reasonable time, then Supplier will refund the amount Customer paid for the affected Equipment as depreciated on a straight-line basis over a 5 year period, upon return of such Equipment to Supplier.

**B. Software Warranty.** The following terms apply to the specific Software ("Warranted Software") listed in the table located at [www.dellemc.com/content/dam/digitalassets/active/en/unauth/manual-warranty-informations/h4276-emc-prod-warranty-maint-table.pdf](http://www.dellemc.com/content/dam/digitalassets/active/en/unauth/manual-warranty-informations/h4276-emc-prod-warranty-maint-table.pdf) (the "Software Warranty Table"), which shall extend to the firmware and associated software drivers for Supplier-branded hardware components which are necessary to allow the Supplier-branded hardware Equipment to meet its published specifications for such period of time as Supplier's warranty on Supplier-branded hardware Equipment is effective. Supplier warrants that Warranted Software will substantially conform in all material respects to its then-current documentation during the applicable warranty period specified in the Software Warranty Table (the "Software Warranty Period"). Any breach of this warranty must be reported to Supplier during the Software Warranty Period. Customer's sole and exclusive remedy and Supplier's entire liability for a breach of this warranty is for Supplier, at its sole discretion, to use commercially reasonable efforts to remedy the non-conformance, or else to terminate the license for the affected Software and provide a pro-rata refund of the license fees received for such Software.

Additionally, to the best of Supplier's knowledge, the Supplier branded software as delivered by Supplier does not contain any virus or malicious code, routines or devices designed specifically to disable, damage, impair, erase, deactivate, or electronically repossess the Supplier branded software or other software or data (all together, "Malicious Code"); For the avoidance of doubt, "Malicious Code" shall not include any license management technology, remote access functionality, or security features provided by Supplier in accordance with the applicable documentation or agreed terms. Provided, however: (i) the Supplier branded software may include software routines designed to permit Supplier (or other person acting by authority of Supplier) to obtain access to Customer's computer system(s) (e.g., remote access) for purposes of the provision of maintenance or technical support; (ii) Reseller may have a software license key/authorization code provided by Supplier in order to enable use of some of the software; and (iii) Supplier may in the future implement license management technology, features and functionality that are included in the Product and described in the applicable documentation that are not covered by the language set forth herein, and such shall not be a violation of this provision. Customer's remedy for breach of this provision shall be the immediate replacement of all copies of the affected software rightfully in the possession of Customer with a copy that does not contain such Malicious Code.

**C. Notice.** Customer must promptly notify Supplier of any warranty claims within the applicable warranty period.

**7.2 Services Warranty.** Supplier will perform Services in a workmanlike manner in accordance with generally accepted industry standards. Customer must notify Supplier of any failure to so perform within 30 days after the date on which such failure first occurs. In such case, Supplier will use reasonable efforts to correct such failure within a reasonable period of time. If, after reasonable efforts, Supplier is not able to correct such deficiencies for reasons for which Supplier is responsible, then Customer may terminate the affected Services for cause by providing written notice to Supplier.

**7.3 Subscriptions Warranty.** During the initial Subscription Term (as that term is defined and discussed in the APEX-Subscriptions document) for an applicable Order, Supplier will exercise reasonable care to maintain a Product's ability to perform substantially in accordance with the corresponding standard documentation issued by Supplier for the applicable Product under normal usage and with regular recommended service, and provide Services in a workmanlike manner. You will promptly provide Supplier and Prime Contractor with written notice of any failure to conform with the foregoing warranty but within thirty (30) days after the date on which such failure first occurs for Services. Supplier's entire liability and Your exclusive remedies for any failure to comply with this warranty are as follows: Supplier will make reasonable efforts to correct the non-conformance within a reasonable period of time, not to exceed 30 days from receipt of Your notice (the "Cure Period"); and (a) if Supplier is unable to correct the non-conformance during the Cure Period for reasons for which Supplier is responsible, then Supplier will replace the non-conforming Product or reperform the applicable Services; or (b) if Supplier, at its sole discretion, determines such is not reasonably possible, then You may terminate the applicable Order and End User Subscription Form and request a refund of any prepaid fees for the Subscription that will not be provided as a result of the termination.

**A. Warranty Limitations for Subscriptions.** The warranties set forth in this clause do not cover problems that arise from: (i) accident or neglect by You or any third party; (ii) any third party items or services with which the Product is used or other causes beyond Supplier's control; (iii) installation, operation or use not in accordance with Reseller's or Supplier's instructions and the applicable documentation; (iv) use in an environment, in a manner or for a purpose for which the Product was not designed; (v) modification, alteration or repair by anyone other than Supplier personnel or its authorized designee or (vi) causes attributable to normal wear and tear (e.g., cosmetic damage that doesn't affect the Product's functionality). Supplier has no obligation for: (1) Software installed or used beyond the licensed use, or (2) Product whose original identification marks have been altered or removed. Products and Services are not fault-tolerant and are not designed or intended for use in hazardous environments requiring fail-safe performance, such as any application in which the failure of the Products or Services could lead to death, bodily injury, or physical or property damage (collectively, "High-Risk Activities").

**B. Warranty Disclaimer for Subscriptions.** Other than the warranties set forth in this clause, and to the maximum extent permitted by applicable law, Supplier: (i) makes no other express warranties; (ii) disclaims all implied warranties, including merchantability, fitness for a particular purpose, title and non-infringement; and (iii) disclaims any warranty arising by course of dealing or performance, or usage of trade. Supplier expressly disclaims any express or implied warranty of fitness for High-Risk Activities. Supplier is not responsible for delays, interruptions, service failures or other problems inherent in use of internet and electronic communications or for issues related to Colocation Sites.

**7.4 General Warranty Limitations.** The warranties set forth in this clause 7 do not cover problems that would not have occurred but for: (i) accident or neglect by Customer or any third party; (ii) any third party items or services with which the Product is used or other causes beyond Supplier's control; (iii) installation, operation or use not in accordance with Supplier's instructions and the applicable documentation; (iv) use in an environment, in a manner or for a purpose for which the Product was not designed; or (v) modification, alteration or repair by anyone other than Supplier personnel or its authorized representatives; or (vi) causes attributable to normal wear and tear. Supplier has no obligation for: (1) Software installed or used beyond the licensed use, or (2) Product whose original identification marks have been altered or removed. Supplier Offerings are not fault-tolerant and are not designed or intended for use in hazardous environments requiring fail-safe performance, such as any application in which the failure of the Offerings would be reasonably likely lead to death, bodily injury, or physical or property damage (collectively, "High-Risk Activities"). Supplier expressly disclaims any express or implied warranty of fitness for High-Risk Activities. Supplier does not warrant an uninterrupted or error-free operation of Software, except as provided in this Section 7, nor that all defects can be corrected.

**7.5 General Warranty Disclaimer.** Other than the warranties set forth in this Section 7 and the Schedules, and to the maximum extent permitted by applicable law, Supplier: (i) make no other express warranties; (ii) disclaim all implied warranties, including merchantability, fitness for a particular purpose, title and non-infringement; and (iii) disclaim any warranty arising by course of dealing or performance or usage of trade.

## **8 Indemnification.**

### **8.1 General Indemnification.**

Supplier shall defend (subject to the consent of the Office of the Attorney General ("OAG")) and indemnify the State, its agencies, officers, employees, and agents (each a "State Indemnified Party" or together, the "State Indemnified Parties") from and against any third-party claims to the extent the claims in any way relate to, arise out of, or result from:

- i. any negligent act, negligent omission, or intentional or willful misconduct of Supplier or any Supplier Personnel for criminal conduct or fraud, damage to tangible property, or injury or death to persons; or
- ii. any claims by any subcontractor resulting from Supplier's failure to pay such Subcontractor. (Each of the above is a "Claim," except that any claims involving actual or alleged infringement of a third party's intellectual property are governed by subsection 8.2, "Indemnification for Intellectual Property Claims," set forth below.)

Supplier will be solely responsible for all costs and expenses associated with the defense of all third-party Claims against State Indemnified Parties. In connection with the defense of a claim by Supplier, selection and approval of counsel, and approval of any settlement shall also be subject to the consent of the OAG.

If a Claim is commenced against any State Indemnified Parties by a third party and Supplier is of the opinion that the allegations in the Claim, in whole or in part, are not covered by this indemnification provision, then Supplier shall immediately notify the State in writing of its opinion. Supplier shall, nonetheless, take all reasonable steps to protect the rights, remedies, and interests of the State Indemnified Parties in the defense of the Claim, including to secure a continuance to permit the State to appear and defend its interests in cooperation with Supplier as is appropriate, including any jurisdictional defenses the State may have.

### **8.2 Indemnification for Intellectual Property Claims.**

Supplier shall defend (subject to the consent of the OAG) all State Indemnified Parties against any third-party claims alleging that use of Supplier-branded Product, Subscription or Support and Professional Services (but excluding Third Party Products) (together, "Covered IP Offerings"), in accordance with this CTS, infringes or

misappropriates a third party's intellectual property rights enforceable in the country(ies) that are signatories to the Berne Convention (each an "**IP Claim**"); and indemnify State Indemnified Parties by paying: (1) the resulting costs, attorney fees, and damages finally awarded against the State Indemnified Parties by a court of competent jurisdiction to the extent that such are the result of the third party IP Claim; or (3) the amounts stated in a written settlement negotiated and approved by Supplier for any IP Claim.

In connection with the defense of an IP Claim by Supplier, approval of counsel, and approval of any settlement shall also be subject to the consent of the OAG. Subject to these limitations, Supplier shall have the right and ability to make any final decisions regarding the resolution of the IP Claim. In the event such an IP Claim results in a settlement between Supplier and the State, Supplier will negotiate with the OAG to agree on a settlement that shall be reasonably satisfactory to the State, provided Supplier shall otherwise have the right and ability to make any final decisions regarding the resolution of the IP Claim.

In the event that an IP Claim is commenced against any of the State Indemnified Parties and Supplier is of the opinion that the allegations in whole or in part are not covered by this indemnification provision, Supplier shall immediately notify the State in writing, specifying to what extent Supplier believes it is obligated to defend and indemnify under the terms and conditions of this CTS. The State may, at its own expense, participate in the defense of any IP Claim and represent its own interests and Supplier shall in such event make commercially reasonable efforts to provide reasonable cooperation to the State to permit the State to defend its interests.

In the event of a IP Claim pursuant to any actual or alleged infringement or misappropriation of any third party's intellectual property rights by any of the affected Covered IP Offerings, and in addition to all other obligations of Supplier in this Section, Supplier may at its expense and discretion, either (a) procure for the State the right to continue use of such affected Covered IP Offerings; or (b) replace or modify the affected Covered IP Offerings with, or any component thereof to make them non-infringing substitutes, which shall have no material reduction in functionality; or if, in Supplier's opinion, neither of the foregoing are reasonably available, Supplier shall reimburse the State for the reasonable costs incurred by the State in obtaining alternative Covered IP Offerings in the event State cannot benefit from such replacements for the affected Covered IP Offerings. If Supplier cannot accomplish any of the foregoing within a reasonable time and at commercially reasonable rates, then Supplier shall accept the return of any infringing component of the Services, along with any other components rendered unusable by the State as a result of the infringement, and provide a pro rata refund for the affected Covered IP Offerings, excluding Subscription Software.

Notwithstanding the foregoing, Supplier shall have no obligation under this subsection where the infringement alleged in any IP Claim would not have occurred but for: (i) any modifications of the Supplier Covered IP Offerings that were not performed by or on behalf of Supplier (or by Reseller); (ii) any combination, operation, or use of a Supplier Covered IP Offerings with any other products, services, items or technology introduced by the State, including third-party products and open-source software; (iii) use for a purpose or in a manner for which the Covered IP Offerings was not designed, or use after Supplier notifies the State to cease such use due to a possible or pending IP Claim; (iv) any modifications made by any person other than Supplier or its authorized representatives or Certified Partners; or (v) Supplier's compliance with the State's written specifications or directions, including the incorporation of any software or other materials or processes provided by or requested by the State.

Supplier's duty to indemnify and defend under this subsection is contingent upon: (i) Supplier receiving written notice of the third-party IP Claim within a reasonable period of time; and (ii) subject to the consent of the OAG and to the extent provided, Supplier having the right to control the defense and resolution of such claim or action, provided that resolution does not require monetary payment by the State without its OAG's consent; and the State's reasonable cooperation with any requests for information by Supplier, at Supplier's expense, in connection with defending and resolving such claim or action.

This subsection provides the State's exclusive remedies for any IP Claim, and nothing in this CTS or elsewhere will obligate Supplier to provide any greater indemnity to the State.

Supplier agrees to extend to the State any warranty or indemnity provided by Dell's suppliers, applicable to any non-Supplier branded Products provided by Supplier to the State under this Agreement, that may by its own terms be extended to the State without additional payment or liability by Supplier.

**8.3 No Indemnification by the State.** Regardless of any language to the contrary elsewhere, the parties acknowledge and agree that in accordance with Article VIII, Section 1(a), (b) of the Constitution of the State of Illinois, the State may not indemnify private parties absent express statutory authority permitting the indemnification. Any language that is inconsistent or conflicts with this section, whether incorporated or referenced within the Dell Terms or elsewhere, is null and void.

#### **8.4 Supplier Notice and Remediation of a Breach or Security Incident.**

A. Following discovery or notification of a Breach (as defined under Section 5 of the Illinois Personal Information Protection Act, 815 ILCS 530 ("PIPA")) or Security Incident (as defined below) that impacts State data, systems, or networks, Supplier shall notify the State in the most expedient time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach. "Security Incident" means any confirmed breach or vulnerability of Supplier's systems, or Products and Services provided under the Dell Terms, that involves destruction, loss, alteration, unauthorized disclosure of, or access to, any State data that is transmitted, stored, or processed by Supplier.

B. After becoming aware, and providing notice to the State under Section 8.4(A), of a Breach or Security Incident relating to the Products or Services provided by Supplier under the Dell Terms, Supplier shall: (i) use reasonable efforts to mitigate the adverse effects of any such Breach or Security Incident; and (ii) use reasonable efforts to promptly remedy any such Breach in accordance with applicable laws, regulations, and industry standards, including but not limited to PIPA, 815 ILCS 530.

C. Subject to the limitations listed in Section 9, Supplier shall also reimburse the State for costs incurred by the State in responding to, and mitigating damages caused by, any such Breach or Security Incident, to the extent such costs are directly related to the Breach or Security Incident, including costs of notice and/or remediation.

### **9 Limitation of Liability.**

**9.1 Limitations on Damages.** The limitations, exclusions and disclaimers stated below apply to all disputes, claims or controversies (whether in contract, tort (including negligence) or otherwise) related to or arising out of the Dell Terms ("Dispute").

**A. Limitation on Direct Damages.** Except for claims of death or injury to persons or real property, claims of fraud or intentional misrepresentation, or Supplier's indemnification and defense obligations under Sections 8.1 ("General Indemnification") and 8.2 ("Indemnification for Intellectual Property Claims"), Supplier's total liability to the State under the Dell Terms is limited to the greater of (i) \$10,000,000.00 (ten million dollars), or (ii) three (3) times the amount paid or payable under the Contract for the specific Product, Subscription and/or service giving rise to such liability. Notwithstanding anything otherwise set forth above, Supplier shall have no liability to the State for any direct damages resulting from the State's use or attempted use of Third Party Software, Free Software or Development Tools, all defined in the EULA, or Third Party Products.

**B. Disclaimer of Certain Other Damages.** Neither Supplier nor Customer has liability to the other for special, consequential, exemplary, punitive, incidental or indirect damages, or for lost profits, loss of revenue, loss or corruption or data (except as specifically provided for in Section 8.4 of this CTS), or loss of use or procurement of substitute products, subscriptions, or services.

**9.2 Prevention and Mitigation.** Customer is responsible for its data. Customer shall implement IT architecture and processes enabling Customer to prevent and mitigate damages in line with the criticality of the systems and data for Customer's business and its data protection requirements, including a business recovery plan. In that regard, Customer shall: (i) provide for a backup process on a regular (at least daily) basis and backup relevant data before Supplier performs any remedial, upgrade or other works on Customer's IT systems; (ii) monitor the availability and performance of its IT environment during the performance of Services; and (iii) promptly react to messages and alerts received from Supplier or through notification features of the Products and promptly report any identified issue to Supplier. To the extent that Supplier has any liability for data loss, Supplier shall only be liable for the cost of commercially reasonable and customary efforts to recover the lost data from Customer's last available backup.

**9.3 Reserved.**

## **10 Third Party Products.**

Only to the extent available under the Contract, Supplier may offer to supply Third Party Products that are provided by a third-party manufacturer /supplier, e. g. under Supplier's "Dell EMC Select" program, Supplier's "Brokerage" program or Supplier's Software & Peripherals (S&P) program, and may include offerings from Supplier Affiliates using different brands other than "Dell" or "Dell EMC". Notwithstanding any other provisions herein, such Third Party Products are subject to the standard license, services, warranty, indemnity and support terms of the third party manufacturer/supplier (or an applicable direct agreement between Customer and such manufacturer/supplier). Regardless of other Support Services, such Third Party Products are not supported by Supplier and Customer shall contact such third party directly for support. Any warranty, damages or indemnity claims against Supplier in relation to such Third Party Products are expressly excluded. References to warranty and support information for Dell EMC Select products is available through [www.dell.com/offeringspecificterms](http://www.dell.com/offeringspecificterms).

## **11 Confidentiality.**

**11.1** Each party, including its Affiliates, agents and subcontractors, may have or gain access to confidential data or information owned or maintained by the other party in the course of carrying out its responsibilities. "Confidential Information" means any information that is (i) exempt from disclosure pursuant to the Illinois Freedom of Information Act (5 ILCS 140) and (ii) marked "confidential" or "proprietary" or, if disclosed orally, is identified as being confidential at the time of disclosure and, within two (2) weeks thereafter, is summarized, appropriately labeled, and provided in tangible form. Confidential Information does not include information that is (i) rightfully in the receiving party's possession without prior obligation of confidentiality from the disclosing party; (ii) a matter of public knowledge; (iii) rightfully furnished to the receiving party by a third party without confidentiality restriction; or (iv) independently developed by the receiving party without reference to the disclosing party's Confidential Information.

**11.2** Each party shall (a) use Confidential Information of the other party only for the purposes of exercising rights or performing obligations in connection with this CTS; and (b) protect from disclosure to any third parties, by use of a standard of care equivalent to that as used by recipient to protect its own information of a similar nature and importance, and, no less than the use of reasonable care, any Confidential Information disclosed by the other party.

**11.3** The obligation of confidentiality will apply for a period commencing upon the date of disclosure until three (3) years thereafter, except with respect to: (1) End User data to which Dell may have access in connection with the provision of Services, which is and shall remain Confidential Information unless and until one of the exceptions stated in the above definition of Confidential Information applies; and (2) Confidential Information that constitutes, contains or reveals, in whole or in part, Dell proprietary rights, which shall not be disclosed by the receiving party at any time.

**11.4** Unless otherwise agreed by the parties, and then only upon receipt of the State's prior written consent, Supplier and its subcontractors shall not access or attain any personally identifiable information or sensitive information on or from the State's systems and Supplier agrees that any such information is the Confidential Information of the State. In any event, each party shall implement and maintain reasonable security measures to protect any and all data, information, and records disclosed by the other party under these Dell Terms from unauthorized access, acquisition, destruction, use, modification, or disclosure.

**11.5** Promptly upon termination of this CTS, or earlier at the written request of the disclosing party, the receiving party will either promptly return any Confidential Information in a non-proprietary format or notify the disclosing party in writing of its destruction. Notwithstanding the foregoing, recipient's professional advisors (e.g., lawyers and accountants) may retain in confidence copies of their respective work papers and final reports in accordance with their professional and ethical obligations. Notwithstanding the foregoing, neither party will be required to search archived electronic back-up files or its computer systems for discloser's Confidential Information in order to purge such Confidential Information from its archived files.

**11.6** The State agrees that if it receives a request for Supplier's information pursuant to FOIA and/or other applicable laws and regulations, the State will make reasonable efforts to provide Supplier with written notice of the request. Subject to the requirements of this Section 11 (Confidentiality), Supplier may disclose Confidential Information (1) to an Affiliate, or to a subcontractor used by Supplier to provide Services under the Dell Terms, as long as the Affiliate or subcontractor has a need-to-know and complies with the foregoing; (2) to Supplier's directors, officers, employees, and professional advisors and those of its Affiliates, and (3) if required by law or regulatory authorities. For the purposes of this present section, "Affiliates" of Supplier include other members of Dell Technologies.

## **12 Data Privacy.**

**12.1** Parties will comply with all data protection laws and regulations applicable to the processing of personal data under this CTS. In this section "personal data", "controller", "processor" and "processing" will have the meaning set out in the applicable data protection legislation. For the avoidance of doubt, the State denies that it has any obligation to comply with any privacy laws other than those enacted by the State of Illinois and the United States federal government or that it has any obligation to comply with the terms of the GDPR, the UK GDPR, the CCPA or other similar law or regulation of any foreign state or jurisdiction.

**12.2** To the extent that Supplier processes any personal data on behalf of Customer in the performance of its obligations under this CTS, Supplier will only do so as required to fulfil its legal obligations pursuant to this CTS and either, as a controller and on its own behalf in accordance with the Privacy Statement, or as a processor acting on behalf of Customer in accordance with the DPA, and within the bounds of the Cloud Storage Area (as defined in the CSOA) for purposes of a Service Offering under the CSOA.

**12.3** **Reserved.**

## **13 Term and Termination of this CTS.**

The CTS is effective upon the last execution of the parties listed below and continues until it is terminated in

accordance with this clause or upon termination of the Contract, whichever happens first. Either party may terminate this CTS for material breach by the other party (excluding all issues related to the timing of payments, which do not constitute a material breach) if such other party has failed to cure the breach within a reasonable grace period of no less than 30 days as set forth by the other party in writing. A termination for convenience shall only be permitted in accordance with the terms of the Contract.

## **14 General.**

**14.1 Governing Law; Jurisdiction.** The CTS and all of the Dell Terms shall be construed in accordance with and governed by the laws and rules of the State of Illinois. Any claim against the State arising out of this CTS or any Dell Terms document must be filed exclusively with the Illinois Court of Claims (705 ILCS 505/1). Regardless of any language elsewhere, the State shall not enter into binding arbitration to resolve any dispute arising out of this CTS or any Dell Terms document. The State of Illinois does not waive sovereign immunity (including all rights provided in the State Lawsuit Immunity Act, 745 ILCS 5) by entering into this CTS or any Dell Terms document.

**14.2 Trade Compliance.** Customer's usage of the Products or Services and access to related technology (the "Materials") are for its own use, not for resale, export, re-export or transfer. The Customer further acknowledges that it will not transfer any Materials to foreign countries and that all transactions under this CTS will occur within the United States.

**14.3 Customer Acknowledgements.** Under this CTS and any Dell Terms document, Customer agrees and acknowledges that it has the right to any technology or data that Customer provides to Supplier. To the extent Reseller and the State may mutually determine the need applies on a per-order basis, they will enter into a SOW to address any: (a) technology or data (including personal data, if applicable) that Customer needs to provide to Supplier to enable Supplier to provide Services, and (b) non-Supplier software or other components that Customer directs or requests that Supplier or Reseller use with, install, or integrate as part of the Supplier's Offerings. Customer agrees and acknowledges that Supplier is not responsible for reviewing data that will be provided to or accessed by Supplier in the provision of the Offerings to ensure that such data does not contain: either (i) data that is classified, ITAR (International Traffic in Arms Regulations) related data, or both; or (ii) articles, services, and related technical data designated as defense articles and defense services.

**14.4 Encryption. For purposes of this section, Supplier is not responsible for reviewing data that will be provided (or to which Supplier will have access). All items (including hardware, software, technology and other materials) provided to Supplier for any reason that contain or enable encryption functions either:**

(a) satisfy the criteria in the Cryptography Note (Note 3) of Category 5, Part 2 of the Wassenaar Arrangement on Export Controls for Conventional Arms (Wassenaar Arrangement) and Dual-Use Goods and Technologies and Category 5, Part 2 of the U.S. Commerce Control List (CCL) or (b) employ key length of 56-bit or less symmetric, 512-bit asymmetric or less, and 112-bit or less elliptic curve or (c) are otherwise not subject to the controls of Category 5, Part 2 of the Wassenaar Arrangement and Category 5, Part 2 of the CCL. Supplier is not responsible for determining whether any third-party product to be used in the products and services satisfies regulatory requirements of the country to which such products or services are to be delivered or performed. Supplier shall not be obligated to provide any product or service where the product or service is prohibited by law or does not satisfy the local regulatory requirements.

**14.5 U.S. Government Restricted Rights.** The software and documentation provided are "commercial products" as defined in Federal Acquisition Regulation ("FAR") Section 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as these terms are used in FAR 12.212 and Defense Federal Acquisition Regulation Supplement ("DFARS") Section 227.7202, as applicable.

Consistent with FAR 12.212 and DFARS Section 227.7202, all U.S. Government end users acquire the software and documentation with only those rights set forth herein.

**14.6 Entire Agreement.** This CTS and the other Dell Terms, as listed above, together with the portions of any Order including Professional Services to be fulfilled by Supplier, comprise the complete statement of the agreement of the parties regarding the subject matter thereof and may be modified only by written agreement.

**14.7 Force Majeure.** Failure by either party to perform its duties and obligations under this CTS or any Dell Terms document will be excused to the extent necessary by unforeseeable circumstances beyond its reasonable control and not due to its negligence, including acts of God, natural disasters, acts of war, terrorism, riots, labor disputes, fire, flood, explosion, governmental prohibition, local or national emergency, epidemics/pandemics, general import/export/customs process problems affecting supplies to Supplier, shortages in materials, failure of a utility service or transport network, embargo, strike, lock out or other industrial dispute. The non-declaring party may cancel an affected order issued under the Contract without penalty if any delay or failure to perform lasts longer than thirty (30) days after notification by the affected party.

**14.8 Assignment and Subcontracting.** Neither party shall assign, transfer or novate this CTS, any Professional Services to be provided by Dell under any Order or any right or obligation thereunder or delegate any performance without the other party's prior written consent, which consent shall not be unreasonably withheld. Notwithstanding the foregoing, (i) Supplier may use Affiliates or other qualified subcontractors to perform its obligations hereunder, provided that the relevant party to the order shall remain responsible for the performance thereof.

**14.9 Independent Contractors.** The parties are independent actors for all purposes under this CTS and cannot obligate any other party without prior written approval. The parties do not intend anything in this CTS to allow either party to act as an agent or representative of the other party, or the parties to act as joint venturers or partners for any purpose. Neither party is responsible for any acts or omissions of the other.

**14.10 Third Party Rights.** There are no third-party beneficiaries to this CTS under any laws.

**14.11 Waiver and Severability.** Failure to enforce a provision of this CTS will not constitute a waiver of that or any other provision of this CTS. If any part of this CTS or an Order is held unenforceable, the validity of the remaining provisions shall not be affected.

**14.12 Notices.** The parties will provide all notices under this CTS and all Dell Terms in writing, subject to this provision. Customer must provide notices to Supplier at the Dell email address on the first page of the CTS. Supplier must provide notices to the State at DoIT.GeneralCounsel@illinois.gov.

The undersigned duly authorized representatives of the parties hereby enter into and execute on their behalf this CTS and the other Dell Terms attached herein as exhibits, all effective as of the last signature below.

**Dell Marketing L.P.**

Printed Name: Katherine Castillo  
Signature: *Katherine Castillo*  
Title: Paralegal Advisor  
Date: 04/07/2025

**The State of Illinois, through the Department of Innovation and Technology**

Printed Name: Brandon Ragle  
Signature: *Brandon Ragle*  
Title: Acting Secretary  
Date: 4/18/2025

Reviewed as to legal clause sufficiency  
DK 04/07/2025

## **Exhibit A:**

### **Dell End User License Agreement**

This End User License Agreement (“EULA”) is between the State of Illinois, through the Department of Innovation and Technology (the “State,” “DoIT,” or “You”) and one of the three following applicable entities (as discussed and further clarified in the “Licensor Table” included at the end of this EULA) (“Licensor”):

- EMC Corporation, located at 176 South Street, Hopkinton, Massachusetts 01748;
- Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930; or
- Dell Products L.P., a Texas Limited Partnership, located at 1 Dell Way, Round Rock TX 78682.

This EULA, entered into together with and included as an exhibit to the Commercial Terms of Sale between You and Dell Marketing L.P. (the “CTS”), governs Your and Your users’ use of (including any third party use permitted under this EULA): (a) the object code version of Dell branded software that is preinstalled on Dell hardware provided to You pursuant to an order through reseller Ahead, Inc. (“Reseller”) under State Contract #CMT4040325 (the “Contract”) between the State and Reseller (each, an “Order”); (b) associated software license keys, if any (“License Keys”); (c) updates to such software (“Updates”); (d) the documentation for such software; and (e) all copies of the foregoing (collectively, “Software”), all in relation to Orders placed under the Contract. This EULA is effective as of the Effective Date of the CTS.

#### **1. License Grant.**

1.1. Right to Use. Subject to the terms and conditions of this EULA, Licensor grants to You a non-exclusive license to use the Software during the period stated in the applicable Order (if no period is specified, You may use the Software perpetually), in connection with the internal business operations of Your entity (which include all State of Illinois governmental operations). In addition, You may make a reasonable number of copies of the Software solely as needed for backup or archival purposes. Additional license terms for certain Software may be included in the Offering Specific Terms Table located at [www.dell.com/offeringspecificterms](http://www.dell.com/offeringspecificterms) (“OST Table”), and additional terms for Software that is licensed to You for a limited time (“Subscription Software”) are located at [www.delltechnologies.com/subscription\\_terms](http://www.delltechnologies.com/subscription_terms) (“Subscription Terms”). Terms applicable for any Third Party Products that may be at issue are as provided in Section 10 of the CTS (“Third Party Products”).

1.2. Third Party Use. You may allow Your contractors (each, a “Permitted Third Party”) to use the Software solely for the purpose of providing services to You, provided that such use is in compliance with this EULA. No State of Illinois governmental entity serviced by DoIT (which are distinct entities from DoIT) shall be considered a third party under this EULA. You are responsible for any Permitted Third Party’s compliance with this EULA and will ensure such compliance by an Permitted Third Party.

1.3. Rights Reserved. The Software is licensed and not sold. Except for the license expressly granted in this EULA, Licensor, on behalf of itself and its affiliates and suppliers, retains all rights in and to the Software and in all related materials (“Works”). The rights in these Works are valid and protected in all forms, media and technologies existing now or hereafter developed. Any use of Works other than as expressly set forth herein is strictly prohibited.

1.4. Ownership. Licensor, on behalf of itself and its affiliates, retains ownership of the Works and all related intellectual property rights. If Software is provided to You on removable media (e.g., CD, DVD or USB drive), You may own the media on which the Software is recorded.

#### **2. License Conditions.**

2.1. You must do the following:

- A. Run the Software only on the hardware for which it was intended to operate, when applicable;
- B. Use License Keys (if applicable) only from Licensor or an authorized Dell License Key provider;
- C. Treat the Software as Confidential Information that constitutes, contains or reveals, in whole or in part, Dell proprietary rights, which shall not be disclosed by the receiving party at any time. For clarification purposes, State data to which Dell may have access in connection with the provision of Services shall remain Confidential Information unless and until one of the exceptions stated in the CTS definition of Confidential Information applies;
- D. Use the Software only on as many computers or devices that You purchased, in such configurations permitted by Dell or Licensor, and/or in accordance with the applicable unit of measure, each as may be specified on Your Order. For Software licensed via a unit of measure, the terms and descriptions of each unit of measure are located at [www.delltechnologies.com/UOM\\_terms](http://www.delltechnologies.com/UOM_terms) ("UOM Terms"), applicable in the form in which that weblink exists at the time an Order is executed. The parties agree that the terms in this weblink are intended to describe and give context to the units of measure utilized in other Dell Terms and documents.
- E. Abide by Section 13.2 ("Trade Compliance") of the CTS;
- F. Comply with all Third Party Terms (as defined in Section 5 below).

2.2. Except as otherwise permitted by this EULA or by mandatory law (meaning a law that the parties cannot change by contract), You must not do the following:

- A. Modify or remove any proprietary notices or markings on or in the Software;
- B. Transfer License Keys to any non-State of Illinois entity;
- C. Download Updates from Licensor or an authorized provider unless You have a valid support agreement;
- D. Install Updates on Enterprise Products (e.g., server, networking, storage, integrated solutions, and data protection appliances) that have gone end of service life unless Licensor otherwise agrees in writing;
- E. Install and operate counterfeit versions of Software (i.e. software provided by anyone other than Dell or an authorized representative of Dell) on Dell hardware;
- F. Violate or circumvent any technological use restrictions in the Software;
- G. Sell, loan, rent, lease, sublicense, distribute, or encumber (e.g., by lien, security interest, etc.) the Software;
- H. Use any trademarks or service marks of Licensor its affiliates or suppliers;
- I. Provide access to the Software or allow use by any third party, other than Permitted Third Parties, without Licensor's prior written consent (third parties do not include State-of-Illinois entities);
- J. Copy (other than allowed in this EULA), republish, upload, post or transmit the Software in any way;
- K. Modify or create derivative works based upon the Software, or decompile, disassemble, reverse engineer, or otherwise attempt to derive source code from the Software, in whole or in part;
- L. Attack or attempt to undermine the security, integrity, authentication or intended operation of the Software;
- M. Use the Software on a service bureau, rental or managed services basis (except for the State's internal use for State governmental purposes);
- N. Create or permit others to create Internet "links" to the Software or "frame" or "mirror" the Software on any other server, wireless or Internet-based device;
- O. Use the Software to create a competitive offering;
- P. Use the Software to create other software, products or technologies unless the Software contains Development Tools as described in Section 7;
- Q. Share or publish the results of any benchmarking of the Software without Dell's prior written consent;
- R. Use the Software for high risk activities, including without limitation online control systems, or use in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, life support, weapons systems or in any other device or system in which function or malfunction of the Software would be reasonably likely to result in death, personal injury or physical or environmental damage;
- S. Use the Software for activities related to weapons of mass destruction, including but not limited to, activities related to the design, development, production or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or support of missile projects, or chemical or biological weapons; and
- T. Assign this EULA, or any right or obligation under this EULA, or delegate any performance, without Dell's

prior written consent, unless You are transferring the Software in accordance with the Transferability Section 3 below. Even if Dell consents to an assignment, You remain responsible for all obligations under this EULA that You incurred prior to the effective date of the assignment.

**3. Transferability.** You may not transfer the Software to a third party (third parties do not include State-of-Illinois entities) without the express written permission of Dell, unless allowed by applicable law stating that transfer may not be restricted (note that a transfer fee may potentially apply; in such event the parties will negotiate in good faith). To the extent any issues arise under this provision, the parties will work together in good faith to find a solution. Any additional costs or fees will require prior internal State approvals, and are subject to and governed by applicable laws and administrative rules, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCs 5/33E-9).

**4. Compliance Verification.** You will: (a) maintain accurate records of the number of Software licenses ordered and deployed; (b) certify to Dell in writing, at Dell's request, the number of Software licenses deployed at that time; and (c) reasonably cooperate in a timely manner with Dell and its auditors if Dell notifies You that it will conduct an audit to confirm Your compliance with this EULA. Licensor will provide the State with reasonable advance notice of such an audit, of no less than 20 business days including a request to schedule any physical visit to State facilities for such purpose, subject to State security policies and procedures. Any such audit will be conducted during the State's normal business hours and will not interfere unreasonably with the State's normal operations. Licensor will bear Licensor's cost of the audit (including any third-party costs Licensor incurs) and may conduct no more than one audit in any twelve-month period. The parties agree to work together in good faith to address and resolve any issues that may arise relating to over-deployment. Any additional costs or fees shall be subject to prior internal State written approvals and the requirements and limitations of applicable laws and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

**5. Third Party Software.** "Third Party Software" is software, including open source software, that is contained in or provided with the Software and is licensed by a third party under its own terms of use ("Third Party Terms"). Third Party Software is governed solely by the applicable Third Party Terms and not by this EULA. Third Party Terms may be provided with the Third Party Software or may be included in the OST Table. To the extent that an Order contains Third party Software, Reseller shall provide the State with notice that Third Party Terms will apply. Terms applicable for any Third Party Products that may be at issue, including Third Party Software, are as provided in Section 10 of the CTS ("Third Party Products"). For certain open source software, the applicable Third Party Terms may entitle You to obtain the corresponding source files. You may find corresponding source files for such open source software at <https://opensource.dell.com/> or in the "About" or "Read Me" file of Software, or other locations that Licensor may specify.

**6. Free Software.** "Free Software" means Software that is provided to You without additional charge (e.g., scripts that enable customer installation; code that enables You to monitor Your use of Dell products; etc.). You may only use Free Software on or with equipment or in the operating environments for which Dell has designed that Free Software to operate. Licensor may terminate any license to Free Software at any time in its sole discretion. You may not transfer Free Software to anyone else.

**7. Development Tools.** If the Software includes development tools, such as scripting tools, APIs or sample scripts (collectively "Development Tools"), and unless there is a separate agreement between You and Dell or Licensor for the Development Tools, You may use such Development Tools to create new scripts and code for the purpose of customizing Your use of the Software (within the parameters set forth in this EULA and in the Development Tools themselves) and for no other purpose.

**8. Evaluation Software.** This EULA does not license use of Software for evaluation purposes ("Evaluation Software") except to the extent these terms may be invoked by the separate license terms and conditions accompanying that Evaluation Software.

**9. Support Services Not Included.** Maintenance and support services for Software are identified in Your Order and will be provided under a separate services agreement.

**10. Termination.** For Subscription Software, this EULA automatically terminates at the end of Your subscription period unless You renew Your rights. Either party may terminate this EULA if the other party commits a material breach of this EULA (excluding all issues related to the timing of payments which shall not constitute a material breach) and fails to cure such breach within thirty (30) days following receipt of notice of the breach. A termination for convenience shall only be permitted in accordance with the terms of the Contract. This EULA will terminate automatically if You breach any of the terms of this EULA and fail to cure such breach within 30 days following notice of the breach. Upon termination, the license(s) granted hereunder will also terminate and You must cease use of the Software and return or destroy all copies of the Software. Licenses that remain in effect shall continue to be governed by this EULA. Except as otherwise agreed by Dell, You will not get a refund from Dell for applicable pre-paid Software license fees if this EULA is terminated. Rights and obligations under Sections of this EULA that, by their nature should survive, will survive termination.

**11. Warranty Disclaimer.** Under this EULA, Licensor provides neither any warranties for the Software nor does it provide support for the Software. Your rights under any warranties and any support entitlements for Software are solely between You and the Reseller or Dell entity from whom You procured the Software and related support, and are defined under the commercial terms agreed between You and such selling entity. Accordingly, except as otherwise offered by Dell, and subject to the language in Section 7.5 of the CTS (“General Warranty Disclaimer”), the Software is provided by Licensor under this EULA “As Is” without any warranties or conditions. Except as provided in Section 7 of the CTS (“Warranty”), Licensor does not warrant uninterrupted or error-free operation of the Software.

**12. Reserved.**

**13. Additional Terms.**

13.1. Reserved.

13.2. Waiver and Severability. Failure to enforce a provision of this EULA will not constitute a waiver of that or any other provision of this EULA. If a court of competent jurisdiction determines that any part of this EULA or document that incorporates this EULA by reference is unenforceable, that ruling will not affect the validity of all remaining parts.

13.3. Modifications. This EULA may only be modified in writing signed by both parties; provided, however, that Licensor may update the non-material terms and conditions of the Licensor Table, the OST Table, the Subscription Terms, and the UOM Terms at any time. Any such changes that Licensor makes will only apply to Orders that occur after Licensor makes such changes. The State acknowledges that in the normal course of business Dell may update the OST Table, the Subscription Terms, and the UOM Terms. In the event of a material change to the Licensor Table, Licensor will provide written notice and the parties will work in good faith to amend the EULA to reflect any such update.

13.4. Reserved.

13.5. Reserved.

13.6. Third Party Rights. Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.7. Reserved.

## Licensor Table

Software Category	Software Description	Licensor (Based on Customer Location)
<b>Client</b>	Dell application software delivered on a Dell client system (e.g. a Dell laptop, desktop, workstation, or tablet) that performs specialized data processing tasks; and Dell system software included with a Dell client system that provides basic hardware functionality and platforms for applications to run (e.g. firmware and BIOS)	<ul style="list-style-type: none"> <li>• <b>Worldwide:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
<u><a href="#">Converged</a></u>	Software that operates only on block products, such as PowerOne, VBlock and VxBlock	<ul style="list-style-type: none"> <li>• <b>North America:</b> EMC Corporation, located at 176 South Street, Hopkinton, Massachusetts 01748</li> <li>• <b>Outside of North America:</b> EMC Information Systems International Unlimited Company, located at Ovens, Co. Cork, Ireland</li> </ul> <p>Note: Cisco is the licensor of Cisco software in Converged products. Cisco software is governed by the Cisco EULA, and not the Dell Technologies EULA. The Cisco EULA is located at: <a href="http://www.cisco.com/go/eula">http://www.cisco.com/go/eula</a>.</p>
<u><a href="#">Data Protection and Recovery</a></u>	Examples include PowerProtect Data Manager and Data Protection Suite, as well as other software that operates only on Dell EMC data protection appliances	<ul style="list-style-type: none"> <li>• <b>North America:</b> EMC Corporation, located at 176 South Street, Hopkinton, Massachusetts 01748</li> <li>• <b>Outside of North America:</b> EMC Information Systems International Unlimited Company, located at Ovens, Co. Cork, Ireland</li> </ul>
<u><a href="#">Edge</a></u>	Dell software intended to automate / secure multicloud edge operations. Examples include Dell NativeEdge	<ul style="list-style-type: none"> <li>• <b>Worldwide:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
<u><a href="#">Hyper-converged</a></u>	Software that operates only on VxRack, VxRack SDDC; VxRack Flex; VxRail	<ul style="list-style-type: none"> <li>• <b>North America:</b> EMC Corporation, located at 176 South Street, Hopkinton, Massachusetts 01748</li> <li>• <b>Outside of North America:</b> EMC Information Systems International Unlimited Company, located at Ovens, Co. Cork, Ireland</li> </ul> <p>Note: Cisco is the licensor of Cisco software in VxRack products. Cisco software is governed by the Cisco EULA, and not the Dell Technologies EULA. The Cisco EULA is located at: <a href="http://www.cisco.com/go/eula">http://www.cisco.com/go/eula</a></p>

	Software that operates only on XC Series and XC Xpress	<ul style="list-style-type: none"> <li>• <b>Worldwide:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
<b>Infrastructure Planning</b>	Workload observation software tools used to assist with diagnostics, migration planning or other like activities. Examples include Live Optics	<ul style="list-style-type: none"> <li>• <b>North America:</b> Dell Products L.P., a Texas Limited Partnership, located at 1 Dell Way, Round Rock TX 78682</li> <li>• <b>Outside of North America:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
<a href="#"><u>Networking</u></a>	Software that operates only on Networking products, including network management software, such as OpenManage Network Manager, and network system software, such as Open Networking and Networking OS	<ul style="list-style-type: none"> <li>• <b>North America:</b> Dell Products L.P., a Texas Limited Partnership, located at 1 Dell Way, Round Rock TX 78682</li> <li>• <b>Outside of North America:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
<a href="#"><u>Server</u></a>	Software that operates only on Server products, including OpenManage Console, OpenManage Automation, and iDRAC	<ul style="list-style-type: none"> <li>• <b>Worldwide:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
<a href="#"><u>Storage</u></a>	Software that operates only on the SC Series Storage products	<ul style="list-style-type: none"> <li>• <b>Worldwide:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>
	Software that operates only on all other Storage products, including Elastic Cloud Storage (ECS); Isilon; IsilonSD Edge; Unity; VMAX; PowerMax, PowerStore; XtremIO	<ul style="list-style-type: none"> <li>• <b>North America:</b> EMC Corporation, located at 176 South Street, Hopkinton, Massachusetts 01748</li> <li>• <b>Outside of North America:</b> EMC Information Systems International Unlimited Company, located at Ovens, Co. Cork, Ireland</li> </ul>
<a href="#"><u>Wyse</u></a>	All Wyse software products including: Wyse Management Suite; Wyse Converter for PC's; Wyse ThinOS; Wyse ThinLinux; Wyse Windows IoT Enterprise; Wyse TCX Suite	<ul style="list-style-type: none"> <li>• <b>Worldwide:</b> Dell Global B.V. (Singapore Branch), the Singapore branch of a company incorporated in The Netherlands with limited liability, located at 2 International Business Park, The Strategy Tower 2, #01-34 Singapore 609930</li> </ul>

<p><a href="#"><u>Telecom Systems Business</u></a></p>	<p>Software developed by Dell's Telecom Systems Business Unit for Communications Service Providers, including Bare Metal Orchestrator</p>	<ul style="list-style-type: none"><li>• <b>North America:</b> EMC Corporation, located at 176 South Street, Hopkinton, Massachusetts 01748</li><li>• <b>Outside of North America:</b> EMC Information Systems International Unlimited Company, located at Ovens, Co. Cork, Ireland</li></ul>
--	---	--

## Exhibit B:

### Cloud Service Offerings Agreement

This Cloud Service Offerings Agreement (the “**CSOA**”) is entered into between Dell Marketing L.P. (“**Dell**”) and the State of Illinois, through the Department of Innovation and Technology (referred to below as “**Customer**”, “**You**”, or the “**State**”), and applies to the Service Offerings, including Evaluation Services, ordered by You through reseller Ahead, Inc. (“**Reseller**”) under State Contract #CMT4040325 (the “**Contract**”) between the State and Reseller (“**Orders**”). This CSOA applies to the State and its End Users. The State and Dell are each a party and together the parties to this CSOA, which is entered into together with and included as an exhibit to the Dell Commercial Terms of Sale (“**CTS**”), along with the other documents listed at the beginning of the CTS (all together, as defined in the CTS—collectively, the “**Dell Terms**”), including the Dell Software End User License Agreement (“**EULA**”), the Cloud Service Offerings Data Processing Addendum (“**DPA**”), the Dell Privacy Statement (“**Privacy Statement**”), and the Dell APEX Subscriptions Terms for Partner End Users-U.S. Public (“**APEX-Subscriptions Agreement**”). Each Service Offering may have a Service Offering Description, which is incorporated into the CSOA by reference. The CSOA is effective as of the effective date of the CTS (“**Effective Date**”).

#### 1. Definitions.

“**Cloud Storage Area**” means the geographic storage area provided by Dell and its suppliers where Customer Content may be stored, which will be located within the contiguous United States for any State Order.

“**Content**” means data (including all text, sound, video, and image files), software (including machine images), and other information.

“**Customer Content**” means Content You load or use on the Service Offering. Customer Content does not include configuration, performance, and/or usage data that Dell collects in connection with the Service Offering.

“**End Users**” means Your customers or other third parties to whom You may provide a service using the Service Offering.

“**Evaluation Service**” means any Service Offering, or a feature or functionality of a Service Offering, that Dell offers on an evaluation or trial basis. If You are participating in a separate Dell technical preview or beta program, then the terms of that program will apply to that preview or beta program.

“**Login Credentials**” means any passwords, authentication keys, or security credentials that enable Customer’s access, management to the Service Offering, or both.

“**Service Level Agreement**” means the then-current version of Dell’s performance commitments, if any, for the Service Offering. If applicable, these will be provided in the Service Offering Description.

“**Service Offering**” means the Dell-branded cloud service offering, which may include software (including microcode, firmware, operating systems or applications) (“**Software**”) used to operate the cloud service offering, specified in Your Order. “Service Offering” may include an Evaluation Service.

“**Service Offering Description**” means the then-current version of the Dell document or portal/web page that describes the Service Offering You ordered; as revised by Dell from time to time.

“**Subscription Term**” means the initial term of Your authorized use of the Service Offering, as set forth in the applicable Order, together with any extension term as specified in any subsequent applicable Order. The initial term begins on the date specified in the Order. For purposes of any on-demand Service Offering, “Subscription Term” means the period during which You have access to the Service Offering, for which You will be billed, as specified in the applicable Order.

“**Third-Party Products**” means hardware, software, products, or services that are not Dell-branded. Third-Party Products are not embedded components of the Service Offering.

## 2. The Service Offering.

2.1 **Scope.** The CSOA applies to Orders for a Service Offering as of the Effective Date. The CSOA will also apply to any subsequent Orders for additional services, features, functionality, and capacity for that same Service Offering during the Subscription Term (“**Subsequent Order**”). Orders for other separate Service Offerings will be governed by the CSOA then in effect and accepted by You at the time of the separate Order.

2.2 **Service Offering Description.** The scope and details of the Service Offering are provided in the Service Offering Description.

### 2.3 **Use and Ownership of the Service Offering.**

- A. **Access and Use.** You may access and use the Service Offering only: (a) during the Subscription Term; (b) for Your internal business purposes (which includes all State of Illinois governmental purposes); and (c) in accordance with the CSOA. Subject to any termination rights available under Section 6 (“Term and Termination”), the State will remain responsible for authorized fees that accrue during the Subscription Term of an Order, regardless of whether the State stops using a Service Offering within that time.
- B. **Software Use.** You may receive Software from Dell, which must be installed in Your environment to enable You to use the Service Offering. If the Service Offering includes Software that is licensed by Dell to You, then You will only use such Software: (i) in connection with Your use of the Service Offering and as provided in the CSOA; (ii) for the Subscription Term; and (iii) in accordance with Dell’s EULA. You must not: (1) resell or rent the use of the Service Offering (excluding all State of Illinois governmental purposes); or (2) use the Service Offering in support of an offering, or for a purpose, which is intended to compete with Dell’s Service Offering business.
- C. **Customer Content.** If Dell believes a problem with the Service Offering is caused by, or results from, Customer Content, or Your use of the Service Offering, then You agree to cooperate with Dell in order to identify and resolve the problem.
- D. **Ownership.** You agree that Dell owns all rights, titles, and interests in and to the Service Offering and all improvements, enhancements, modifications, and derivative works, and all intellectual property rights in all of these. Your rights to use the Service Offering are limited to those specifically stated in writing in the CSOA. You agree that You do not have any other implied rights in, or to, the Service Offering. Dell reserves all rights not granted to You in the CSOA.

## 3. Modifications.

3.1 **Generally.** Dell may modify the Service Offering from time to time. Modifications may include optional new features for the Service Offering, which You may use subject to the then-current Service Offering Description or changes to components of the Service Offering. Dell will give You notification of material modifications, including their effective date, either by email, through a portal as applicable, or directly through the Service Offering. Except as addressed by Section 3.2 (Material Modifications) below, Your continued use of the Service Offering after the date of any modification will be considered as Your acceptance of the modified Service Offering.

### 3.2 **Material Modifications.**

A. **Option to Terminate.** If Dell removes a material feature or materially reduces the functionality of the Service Offering, then Dell will notify you by the Notice provision of the CTS, as well as through the relevant portal or by email and You will have the right to terminate the Order for the Service Offering by notifying Dell within 30 days from the date of Dell’s modification notice. If You elect to terminate that Order, then termination occurs on: (a) the date Dell receives Your notice of termination; or (b) any later date You specify in Your notice (though this date must not occur more than 90 days after the date Dell receives Your termination notice).

B. **Right to Refund.** You remain responsible for all fees authorized by an Order that are incurred through the termination date. Dell will promptly refund any prepaid fees for the Service Offering that will not be provided as a result of the termination by You under Section 3.2.A (Option to Terminate).

## 4. Reserved.

## 5. Temporary Suspension.

5.1 **Generally.** Dell may temporarily suspend all Service Offerings subject of a current Order: (a) if You are in material breach of the CSOA (excluding all issues related to timing of payments) and have not cured that breach within 30 days from Dell's notice; or (b) with immediate effect if You breach Dell's Acceptable Use Policy ([www.dell.com/auptranslations](http://www.dell.com/auptranslations)), including all Dell updates to the Acceptable Use Policy during the Subscription Term ("**AUP**") or (c) as provided in the Service Offering Description in effect at the time of the Order. Dell will give You notice before suspending the Service Offering(s) if permitted by law or unless Dell reasonably believes that providing notice presents a risk of harm to the Service Offering(s), to other users of the Service Offering(s), or to any person or property, in which case, Dell will notify You as soon as feasible or permitted. Dell will use best efforts to suspend Your access only to the Service Offering that is the subject of the issue giving rise to the suspension; however, if suspension only to the affected Service Offering is not possible, then Dell is allowed to suspend all the Service Offering(s). The parties will work together in good faith to resolve any such potential issues that may arise, and Dell will promptly reinstate the Service Offering(s) once Dell agrees that the issue(s) causing the suspension has been resolved.

5.2 **Effect of Temporary Suspension.** The State will remain responsible for all applicable fees authorized in an Order that are incurred before and during any suspension. You will not be entitled to any service credits under an applicable Service Level Agreement during any suspension.

5.3 **Termination for Suspension.** If Dell has the right to suspend the Service Offering(s) under Clause 5.1(b) (Suspension - Generally), then Dell also has the right to terminate the Service Offering(s): (a) immediately upon written notice to You in the event of a material breach of the AUP; or (b) as provided under Clause 6.2(c) (Termination) provided that the 30 day cure period is considered to start from the date of Dell's first notice under Clause 5.1(a) (Suspension, Generally).

## 6. Term and Termination.

6.1 **CSOA Term.** This CSOA commences on the Effective Date of the CTS and continues until terminated in compliance with this Clause.

6.2 **Reserved.**

6.3 **Effects of Termination.**

A. **Generally.** When the Service Offering expires, terminates, or is rejected for any reason, You must: (a) stop using the Service Offering; and (b) return or, if requested by Dell, destroy, any of Dell's Confidential Information in Your possession or under Your control (other than information that applicable law requires You to retain). The Service Offering Description will state when Dell will delete any Customer Content. You are responsible for making sure that You have copies of all Customer Content You require prior to the date of any termination.

B. **Refunds.** You may be entitled to a refund of pre-paid fees for the Service Offering that will not be provided as a result of a termination in the following cases: (a) If Dell terminates the Service Offering under Clauses 8.1(b) ("Service Offering Limited Warranty") of this CSOA or Section 8 ("Indemnification") of the CTS; and/or (b) If You terminate the Service Offering under Clause 3.2 ("Material Modifications") of this CSOA or Section 13 ("Term and Termination of this CTS") of the CTS. Any other termination/rejection of the Service Offering will not entitle You to any refunds, credits, or exchanges.

C. **Survival.** The provisions relating to the DPA (as defined in Clause 12.2 (Data Processing)) so long as Dell continues to process Your "**Personal Data**" (as defined in the DPA), all rights of action accruing prior to termination, along with any other provision of the CSOA that, expressly, or by its nature and context, is intended to survive, will survive termination.

## 7. Support Services.

7.1 **Generally.** The Service Offering includes the support and maintenance services described in the Service Offering Description ("**Support Services**"), if applicable.

7.2 **Access to Customer Content.** When providing Support Services, Dell will not access or use any Customer Content unless You have authorized Dell to do so.

## 8. Reserved.

**9. Reserved.**

**10. Evaluation Use.** If You use any Evaluation Service, the terms of this Section 10 govern that use, and control over any conflicting provision of this CSOA. The term “Service Offering” includes an Evaluation Service in all provisions of this CSOA that are not in conflict with the provisions of this Section 10. This section does not apply to Service Offerings before they become generally available.

A. You may use an Evaluation Service only (a) for internal testing and evaluation or trial purposes, and (b) for a period of 30 days (unless Dell specifies otherwise) beginning on the date Dell provides You Login Credentials for or access to the Evaluation Service. You will not have access to the Evaluation Service or to any data or Content in the Evaluation Service after Your authorized use period ends.

B. Use of an Evaluation Service may be subject to additional terms from a third-party service provider.

C. You may use the Service Offering Description provided with an Evaluation Service solely in support of Your authorized use of the Evaluation Service.

D. Dell may provide the Evaluation Service for a particular Service Offering: (a) “AS IS” and (b) without indemnification, warranty, or condition of any kind. No service level commitment will apply to the Evaluation Service.

E. The Data Processing Addendum does not apply to Your use of (i) an Evaluation Service or (ii) any feature within an Evaluation Service, that is not generally available to Dell’s customers.

F. You must not put production data or data regulated by law or regulation into an Evaluation Service. If You put that data into an Evaluation Service, You do so at Your own risk and Dell will not be responsible for the consequences of that use.

G. Certain features or functionality of a Service Offering may not be available in an Evaluation Service. Providing any Evaluation Service, or any feature or functionality in an Evaluation Service, does not constitute Dell’s commitment to offer the Evaluation Service or that feature or functionality on a generally available basis.

H. Dell may modify or terminate an Evaluation Service at any time, and any modification or termination will not be deemed a material, detrimental change.

I. The aggregate liability (excluding indirect damages, for which Dell expressly disclaims all liability) of Dell, and its affiliates and suppliers, for any claim arising from Your use of an Evaluation Service will not exceed \$5,000 USD (or the equivalent in local currency).

**11. Third-Party Offerings.** Dell may offer Third-Party Products, in line with Section 10 of the CTS (“Third-Party Products”) that interoperate with the Service Offering through Dell’s then-current Third-Party Product resale programs (e.g. “Extended Technologies Complete”, “Software & Peripherals (S&P)”). Dell may suspend or terminate provision and hosting of any Third-Party Offerings at any time, and that suspension or termination will not be deemed a material change to the Service Offering for the purpose of Clause 3.2.A (Option to Terminate).

**12. Data Protection.**

**12.1 Security Measures.** Together with Section 9.2 of the CTS (“Prevention and Mitigation”), and without limiting Dell’s obligations under this Data Protection Clause, Dell will provide the Service Offering in compliance with reasonable and appropriate security measures stated in the Information Security Measures Addendum, posted at [https://i.dell.com/sites/csdocuments/Legal\\_Docs/en/us/cloudservices-infosecuritymeasures.pdf](https://i.dell.com/sites/csdocuments/Legal_Docs/en/us/cloudservices-infosecuritymeasures.pdf) (which shall not impose any legal obligations on the State), including all updates during the Subscription Term (“ISMA”). The ISMA and the applicable Service Offering Description define the administrative, physical, technical and other safeguards applied to Customer Content residing in the Service Offering.

**12.2 Data Processing.** The Service Offering will process and store Customer Content in the Cloud Storage Area except as necessary to comply with applicable law or a valid binding order of a law enforcement agency. In the event that Service Provider has the capability and desires to change the location of the Cloud Storage Area for a Customer Site, Service

Provider agrees to promptly notify Customer in writing and provide all relevant details of the desired change to the location of the Cloud Storage Area, and not change the location of the Cloud Storage Area without Customer's prior written approval, which Customer may withhold in its sole discretion. If applicable for the Cloud Storage Area chosen by Customer, the terms of the DPA describes the parties' respective roles for the processing and control of Personal Data that You may provide to Dell as part of the Service Offering. Dell will act as Your authorized data processor in respect of the data processing activities related to the Service Offering, as specified in the CSOA, the DPA and the Service Offering Description. You are responsible for providing any necessary legal notices to your personnel and/or End Users and obtaining any legally required consents related to Your use, collection, disclosure, sharing, cross border data transfer, and processing of Personal Data.

12.3 **Required Disclosures.** If Dell is required by a government body or court of law to disclose any Customer Content, Dell will provide You with notice and a copy of the demand as soon as practicable, unless prohibited by applicable law. Dell will take reasonable steps at Your expense to contest any required disclosure if requested by You.

13. **Reserved.**

14. **Monitoring & Telemetry.** The Service Offering monitors and collects telemetry data relating to Your use thereof, as provided in Section 2.3 ("Telemetry Notice") of the APEX-Subscriptions Agreement. Dell may collect certain information related to the Service Offering through a telemetry collector ("**Collector**"). ("**System Data**" or "**Telemetry Data**").

By utilizing the Service Offering, Customer permits Dell to use the Collector to collect and use System Data for the following purposes ("**Permitted Purposes**"):

- to provide Customer with the Service Offering, including to fulfill applicable warranty and support obligations, and to remotely monitor performance and modify Service Offering configurations;
- to provide either end Customers or Dell Channel Partners (as defined below) with metrics regarding anonymized Service Offering usage and consumption patterns and as specified in the Service Offering Description;
- for sales and marketing, including sales and marketing research; and
- to secure and protect Dell's assets, rights and interests, including where appropriate to investigate, prevent, or take action regarding suspected illegal activity or fraud;
- to comply with Dell's legal obligations, including in response to a court order, warrant, subpoena, regulatory or other legal process; and
- for provision, research, support, or enhancement of Dell products, services and offerings.

Customer agrees that Dell may share the System Data with the following categories of third-parties for the Permitted Purposes:

- Dell third-party service providers; and
- Dell channel partners, including but not limited to resellers, distributors, channel service partners, and OEM partners (collectively, "**Dell Channel Partners**").

Dell owns all anonymized System Data ("**Dell System Data**"). Dell System Data will not contain any personal information, and will be de-identified such that it will not disclose the identity of Customer to any third party. Such obligations shall survive the expiration or termination of the CSOA. Customer acknowledges and agrees that the Collector and Dell System Data is Dell's Confidential Information. Nothing herein grants Customer a license, express or implied, by estoppel, inducement, or otherwise, to use the Collector for any purpose.

15. **Reserved.**

16. **Reserved.**

17. **Reserved.**

**Exhibit C:**  
**Data Processing Addendum**

This Data Processing Addendum (“**DPA**”) to the Agreement shall apply where the provision of cloud services offerings under the Cloud Service Offerings Agreement (the “**Service Offerings**”) by **Dell** to the State of Illinois, through the Department of Innovation and Technology (“**You**”, “**Customer**” or the “**State**”), in connection with an order for such Service Offerings through reseller Ahead, Inc. (“**Reseller**”) under State Contract #CMT4040325 (the “**Contract**”) between the State and Reseller (each, an “**Order**”) to the extent that such Service Offerings involves the Processing of Personal Data which is subject to Privacy Laws where Dell acts as Processor on behalf of the Customer as the Controller. This DPA does not apply where Dell is the Controller. The State and Dell are each a “**party**” and together the “**parties**” to this DPA, which is entered into together with and included as an exhibit to the Dell Commercial Terms of Sale (“**CTS**”), along with the other documents listed at the beginning of the CTS (all together, as defined in the CTS—collectively, the “**Dell Terms**”), including the Cloud Service Offerings Agreement.

**1. Definitions.**

Terms not defined herein have the meanings set forth in the Agreement. The following words in this DPA have the following meanings:

- 1.1 “**Agreement**” means the Cloud Service Offerings Agreement.
- 1.2 “**Controller**” means an entity which, alone or jointly with others, determines the purposes and means of the Processing of the Personal Data.
- 1.3 “**GDPR**” means the General Data Protection Regulation (EU) 2016/679.
- 1.4 “**Model Clauses**” means the Standard Contractual Clauses for the transfer of personal data (Decision 2021/914/EU), as they may be amended or replaced from time to time, in respect of transfers from the European Economic Areas (“**EEA**”) to countries outside the EEA (including the United Kingdom (“**UK**”)) and means the Standard Contractual Clauses for the transfer of personal data to Processors (Decision 2010/87/EU) in respect of transfers from the UK to countries which are not subject to an adequacy decision under UK GDPR.
- 1.5 “**Personal Data**” means any information relating to an identified or identifiable natural person which is Processed by Dell in the performance of the Agreement.
- 1.6 “**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data Processed under this DPA.
- 1.7 “**Privacy Laws**” means any data protection and privacy laws to which a party to this Agreement is subject and which are applicable to the Service Offering provided, including where applicable, the GDPR, UK GDPR, the California Consumer Privacy Act (“**CCPA**”) and other similar laws.
- 1.8 “**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.9 “**Processor**” means an entity which Processes the Personal Data on behalf of the Controller.
- 1.10 “**Subprocessor**” means any Processor engaged by Dell for the provision of the Service Offering.
- 1.11 “**UK GDPR**” means the GDPR as retained under United Kingdom domestic law further to the exit of the UK from the European Union, to be read alongside the UK Data Protection Act 2018, as may be amended from time to time.

**2. Processing of Personal Data.**

**2.1 Roles of the Parties.**

Dell may Process Personal Data under the Agreement as a Processor acting on behalf of the Customer as the Controller.

**2.2 Instructions.**

Dell will Process Personal Data in accordance with Customer’s documented instructions. Customer agrees that

this DPA, the Agreement and any subsequent statements of work or service orders, and any configurations by Customer or its authorized users, comprise Customer's complete instructions to Dell regarding the Processing of Personal Data. Any additional or alternate instructions must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Dell is not responsible for determining if Customer's instructions are compliant with applicable law. However, if Dell is of the opinion that a Customer instruction infringes applicable Privacy Laws, Dell shall notify Customer as soon as reasonably practicable and shall not be required to comply with such infringing instruction. Neither Dell nor any Subprocessor shall be liable for any claim brought by Customer or a third party arising from any action or omission by Dell and/or Subprocessors to the extent such action or omission resulted from compliance with Customer's instructions.

### 2.3 Details of Processing.

Details of the subject matter of the Processing, its duration, nature and purpose, and the type of Personal Data and data subjects are as specified in the Agreement and Annex 1.

### 2.4 Compliance.

Customer and Dell agree to comply with their respective obligations under Privacy Laws applicable to the Personal Data that is Processed in connection with the Service Offering. Customer has sole responsibility for complying with Privacy Laws regarding the lawfulness of the Processing of Personal Data prior to disclosing, transferring, or otherwise making available, any Personal Data to Dell.

## 3. Subprocessors.

### 3.1 Use of Subprocessors.

Dell may use Subprocessors with the Customer's general or specific written consent. Customer agrees that Dell may appoint and use Subprocessors to process the Personal Data in connection with the Service Offering provided that Dell puts in place a contract in writing with each Subprocessor that imposes obligations that are: (i) relevant to the services to be provided by the Subprocessors and (ii) materially similar to the rights and/or obligations imposed on Dell under this DPA. Subprocessors may include third parties or any member of the Dell group of companies. Where a Subprocessor fails to fulfil its data protection obligations as specified above, Dell shall be liable to the Customer for the performance of the Subprocessors' obligations.

### 3.2 List of Subprocessors.

A list of Subprocessors that Dell engages to support the provision of the Service Offering is made available by Dell on [www.dell.com/subprocessors](http://www.dell.com/subprocessors).

## 4. Security.

### 4.1 Technical and organisational security measures.

Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the Processing, and any other relevant circumstances relating to the Processing of the Personal Data on Dell systems, Dell shall implement appropriate technical and organizational security measures to ensure security, confidentiality, integrity, availability and resilience of processing systems and Service Offering involved in the Processing of the Personal Data are commensurate with the risk in respect of such Personal Data. Customer agrees that the technical and organisational security measures described in the Agreement provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause. Dell will periodically (i) test and monitor the effectiveness of its safeguards, controls, systems and procedures and (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Data. Customer is responsible for implementing, configuring and maintaining privacy and security measures for services and products that Customer provides or controls.

### 4.2 Technical Progress.

The Information Security Measures (available at <https://www.dell.com/en-us/lp/legal/soa-infosecuritymeasures>) are subject to technical progress and development and Dell may modify these provided that such modifications do not degrade the overall security of the Service Offering provided under the Agreement.

### 4.3 Access.

Dell shall ensure that persons authorized to access the Personal Data (i) have committed themselves to

confidentiality or are under an appropriate statutory obligation of confidentiality and (ii) access the Personal Data only upon documented instructions from Dell, unless required to do so by applicable law.

## **5. Personal Data Breach.**

Dell will notify the Customer without undue delay after becoming aware of a Personal Data Breach in relation to the Service Offering provided by Dell under the Agreement and will use reasonable efforts to assist the Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

## **6. International Transfers.**

Except for and subject to the restrictions of a contrary Cloud Storage Area, Dell is authorized, in connection with the provision of the Service Offering, or in the normal course of business, to make worldwide transfers of Personal Data to its affiliates and/or Subprocessors. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with this Agreement. Where the provision of Service Offering involves the transfer of Personal Data from the European Economic Area (“EEA”) or the UK to countries outside the EEA or the UK (which are not subject to an adequacy decision under Privacy Laws) Dell agrees it will use the Model Clauses along with appropriate supplemental measures or other appropriate data transfer mechanisms in accordance with applicable Privacy Laws.

## **7. Deletion of Personal Data.**

Upon termination of the Service Offering (for any reason), the parties agree to adhere to data deletion mechanism as set out in the Agreement.

## **8. Cooperation.**

### **8.1 Data Subject Requests.**

Dell shall promptly inform Customer of any requests from individuals exercising their data subject rights under Privacy Laws. Customer is responsible for responding to such requests. Dell will reasonably assist Customer to respond to data subject requests to the extent that Customer is unable to access the relevant Personal Data in the use of the Service Offering. Dell reserves the right to charge Customer for such assistance if the cost of assisting exceeds a nominal amount.

### **8.2 Third party requests.**

If Dell is required by a subpoena, court order, agency action, or any other legal or regulatory requirement to disclose any Customer’s Personal Data, Dell will provide Customer with notice and a copy of the demand as soon as practicable, unless Dell is prohibited from doing so pursuant to applicable law. If Customer requests, Dell will, at Customer’s expense, take reasonable steps to contest any required disclosure.

### **8.3 Privacy Impact Assessment and Prior Consultation.**

To the extent required by Privacy Laws, Dell shall provide reasonable assistance to Customer to carry out a data protection impact assessment in relation to the Processing of Personal Data undertaken by Dell and/or any required prior consultation(s) with supervisory authorities. Dell reserves the right to charge Customer a reasonable fee for the provision of such assistance.

## **9. Demonstrating Compliance.**

Dell agrees to supply, upon Customer request for an audit, the Standardized Information Gathering (“SIG”) questionnaire (“**Security Questionnaire**”) related to the security practices and posture of Dell’s organization. The Security Questionnaire is reviewed annually, mapped to Dell policies and standards, and updated with relevant and current US and international regulatory and privacy standards, such as, NIST 800-53r4, NIST CSF 1.1, CIS Top 20, or ISO 27001, where applicable. To the extent Customer’s audit requirements under the Standard Contractual Clauses or applicable Privacy Laws cannot reasonably be satisfied through the Security Questionnaire, documentation or compliance information Dell makes generally available to its customers, Dell will promptly respond to Customer’s additional audit instructions. Before the commencement of an audit, Customer and Dell will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Dell to unreasonably delay performance of the audit. To the extent needed to perform the audit, Dell will make the processing systems, facilities and supporting documentation relevant to the processing of Personal Data by Dell available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Dell, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Dell’s other customers or to Dell systems or facilities not involved in the Service Offering. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Dell expends for any such audit, in addition to the rates for services performed

by Dell. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Dell and Dell shall promptly cure any material non-compliance.

## **10. CCPA.**

If Dell is Processing Personal Data within the scope of the CCPA, Dell will Process Personal Data on behalf of Customer and will not retain, use, or disclose that Personal Data for any purpose other than for the purposes set out in the DPA and as permitted under the CCPA. In no event will Dell sell any Personal Data.

### **Annex 1 Data Processing Description**

#### **1. Subject matter and duration of the Processing.**

The subject matter and duration of the Processing shall be according to the Agreement.

#### **2. Purpose of Processing.**

Personal Data will be Processed for the purpose of providing Service Offering, as relevant and defined by the selected service levels and support options. The Agreement and the relevant Service Offering descriptions and statements of work ("**Service Offering Descriptions**") shall apply for the specifics and possible additional services.

#### **3. Nature of Processing.**

The nature of the Personal Data Processed is described in the relevant Service Offering Descriptions and statements of work.

#### **4. Categories of Data Subjects.**

The data subjects are Customer's end users, employees, contractors, suppliers and other third parties relevant to the Service Offering.

#### **5. Types of Personal Data.**

The type of Personal Data that may be submitted by the Customer are described in the relevant Service Offering Descriptions and statements of work. Unless otherwise specified, Dell does not Process Special Categories of Data, and Customer shall not provide Special Categories of Data, Personal Health Information, or other similar Personal Data.

## **Exhibit D:**

### **APEX Subscriptions Terms for Partner End Users – U.S. Public**

These Dell APEX Subscriptions Terms for Partner End Users – U.S. Public (the “APEX-Subscriptions Agreement” or “ASA”) establish the terms and conditions between Dell (as defined below in Section 8) and the State of Illinois, through the Department of Innovation and Technology (the “State,” “You,” or “Customer”) that apply to any Subscription for Products or Services that is placed in an order with reseller Ahead, Inc. (“Reseller”) under State Contract #CMT4040325 (the “Contract”) between the State and Reseller (each, an “Order”). The State and Dell are each a party and together the parties to this APEX-Subscriptions Agreement, which is entered into together with and included as an exhibit to the Dell Commercial Terms of Sale (“CTS”), along with the other documents listed at the beginning of the CTS (all together, as defined in the CTS—collectively, the “Dell Terms”), including Exhibit A: the Dell Software End User License Agreement (“EULA”). Capitalized terms used in this APEX-Subscriptions Agreement are defined in the CTS, or throughout this APEX-Subscriptions Agreement or below in Clause 8 (Definitions).

#### **1. Delivery, Site, Use, Risk, and Return.**

**1.1 Delivery; Site.** Reseller will ship the Products to the Site stated in the Order. Where software is provided in a form that is embedded on the Equipment, Reseller will enable any required license keys by electronic means. On or before arrival of the Products to the Site and during the Subscription Term, You shall arrange: (i) appropriate space at the Site; (ii) the necessary environment (power, cooling, etc.) required to support and operate the Products; and (iii) servers and network connectivity required to support Products. The Products may not be moved from the Site without Reseller’s prior written consent, which will not be unreasonably withheld. You grant or will obtain the right for Reseller’s and Dell’s reasonable access to the Site for purposes of: (i) providing Services; (ii) metering; (iii) inspecting the Products; (iv) performing Asset Recovery; and (v) exercising Reseller’s and Dell’s other rights set forth in this Agreement. In case the Equipment is installed at a Colocation Site, You will ensure that both Reseller and Dell are able to exercise their respective rights under this APEX-Subscriptions Agreement concerning the Products stated above. Dell is not responsible for issues generally relating to any Customer Colocation Site.

**1.2 Title.** Dell retains title to Products at all times notwithstanding the manner in which such may be attached or affixed to realty.

**1.3 Use.** You are granted a non-exclusive, non-transferable license to use the Software and the Documentation during the Flexible Consumption Period, and You may use the Products at the Site (or elsewhere, if moved in accordance with Section 1.1 above) only during the Subscription Term, for your internal business operations (which shall include all State governmental purposes generally). Your rights to use the Products provided by Reseller during the Subscription Term are governed by the terms of this APEX-Subscriptions Agreement and, for Software, the terms of the EULA.

**1.4 Third Party Products.** To the extent available under the Contract, Third Party Products are governed by Section 10 of the CTS. Unless otherwise provided in your license agreement with the third-party manufacturer/supplier, You acknowledge that your right to use the Third Party Products is limited to the Subscription Term and any agreed upon extension thereto in accordance with this Agreement.

**1.5 Services.** Scope and the details of Services and Product-specific terms are specified in the applicable standard service description that is referred in the End User Subscription Form. Such standard descriptions are from time to time referred to as “Service Description(s)”, “Product Notices” or “Service Briefs.” The version of the applicable document that is effective as of the date of the applicable End User Subscription Form, is deemed incorporated into this APEX-Subscriptions Agreement. Scope and details of customized Professional Services, if any, not covered by such a standard description will be documented in a mutually agreed Statement of Work (“SOW”). You agree that failure to comply with this APEX-Subscriptions Agreement, including the applicable standard service description and the End User Operating Environment Warranty, may limit Reseller’s ability to provide Services. In such case, proactive support capabilities, response times or other service levels may no longer apply, pending a recertification that may be necessary for continued support. In the event such issues may arise, the parties will work together in good faith to address and resolve the situation. Any additional fees shall be subject to prior internal State of Illinois written approvals and the requirements and limitations of applicable laws and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).

**1.6 Ownership of Customer Content.** You agree that: (i) Customer Content remains the responsibility of Customer; and (ii) neither Reseller nor Dell handles, processes or directs the use of Customer Content.

**1.7 Return of Products; Data Migration.** Prior to any Return of Products, including in case of expiration or termination of the corresponding Schedule, You must: (i) migrate and erase (by method that does not cause damage to the Products) Customer Content from the Products and (ii) establish a mutually convenient date to make the Products available to Reseller or Dell for Asset Recovery, not later than 10 business days from the end of the Subscription Term, except as otherwise may be agreed in writing by the parties. Unless Reseller or Dell have agreed in writing to perform data migration, Reseller and Dell are not responsible for removing Customer Content from the Products. Otherwise, if You have not deleted Customer Content from the Products prior to Asset Recovery, it may be deleted by Reseller or Dell, and the State is solely responsible, and Dell shall not be responsible for, any Customer Content that is not erased or removed from the Products before Asset Recovery occurs.

## **2. Metering.**

### **2.1 Authorization to Meter; Subscription Usage.**

During the Subscription Term, Dell meters usage and collects telemetry data relating to the Products as further provided in Section 2.3 (“Telemetry Notice”). Customer authorizes Dell to meter and/or audit the usage to calculate the associated fees as detailed in the associated Order Schedule. Dell may conduct such activity via electronic means in accordance with Section 2.3 or through on-site inspection (subject to written request made reasonable in advance, and subject to State approvals, scheduling needs, and applicable security policies and restrictions) by Dell personnel and do so only in order to provide support, maintenance, authenticate Customer as the user of the Flexible Consumption and verify Customer’s usage levels. Reseller and Dell shall cooperate with You to minimize the impact of any Dell or Reseller on-site inspection to Your operations.

You agree that:

- A.** Dell may store at the Site, or load onto Products used for electronic communications, such equipment and programming as may be needed by Dell or Reseller solely to track usage levels or perform any reasonable Support Services for Products (“Measuring Equipment”);
- B.** Dell may have reasonable access to the Measuring Equipment at the Site (subject to the above State approvals and restrictions);
- C.** You will provide and maintain equipment (a physical server or virtual machine) necessary to run storage metadata telemetry collection software and enable electronic communications between the Products and Dell;
- D.** You will not disable, interfere in the operation of the Measuring Equipment, or copy or make any use of the Measuring Equipment whatsoever;
- E.** You will protect the Measuring Equipment from disclosure to a third-party; and
- F.** You must, as soon as reasonably possible, install and make available for use all Products contained in each Order including all components that Dell ships to Your Site (e.g., hard drives, etc).

You acknowledge that Dell shares metering information including the Monthly Commitment and Reserve Usage with Reseller for its billing purposes.

### **2.2 Interruption of Metering Capabilities.**

During the Subscription Term, Dell meters usage and collects telemetry data relating to the Products as further provided in Section 2.3. Unless otherwise mutually agreed by Dell and the State in a writing attached to an Order, these terms on the Interruption of Metering Capabilities shall apply. If, for more than ten (10) consecutive days of any calendar month, Dell is unable to monitor usage due to: (i) a failure, act, or omission by Customer, including its personnel and/or third party contractors, or (ii) a failure of any communications equipment used for facilitating metering, then usage will be deemed equal to the usage during the previous

Billing Period. If Dell is unable to meter for a period of more than sixty (60) days due to (i) or (ii), or failure to comply with Section 2.1 (“Authorization to Meter; Subscription Usage”) of this APEX-Subscriptions Agreement, usage for the affected Billing Period(s) will be deemed to be equal to the maximum capacity of the Products. If Dell is unable to meter usage due to any failure which is caused by Dell (e.g., failure of the Measuring Equipment), usage for the affected Billing Period will be deemed to be equal to the Monthly Commitment. Dell will promptly notify the State of an inability to access the Products (electronically or physically, as applicable) and work cooperatively to reestablish access.

**2.3 Telemetry Notice.** Dell collects data from the Products relating to Product location, utilization, configuration, diagnostics and performance, solely for the purpose of providing the Support Services and forecasting capacity requirements (“Telemetry Data”). Telemetry Data does not include any production data stored or processed by Customer on or with a Product or Service, and Dell does not otherwise access, view, process, copy, modify or handle, Customer Data stored on the Products. Notwithstanding the foregoing, Dell will treat any Customer personal data inadvertently collected in accordance with Exhibit E of the CTS, Dell U.S. Privacy Statement. Customer consents to Dell’s collection and use of Telemetry Data for the purposes stated herein.

**3. Reserved.**

**3.1 End User’s Operating Environment.** You agree to operate the Products: (i) with reasonable care, (ii) in accordance with the documentation and configuration provided by Reseller and/or Dell, and (iii) in accordance with industry standards (including but not limited to maintaining a regular data back-up system for Customer Content). You must give prompt written notice of any attachment or judicial process affecting the Products or Dell’s ownership of which You become aware.

**4. Term and Termination.**

**4.1 Term.** This APEX-Subscriptions Agreement is effective on the Effective Date of the CTS and continues until the earlier of termination or Asset Recovery.

**4.2 Effects of Termination.**

**A. Generally.** When the Subscription expires, terminates or is rejected for any reason, You must: (a) stop using the Products; and (b) make the Products available for Asset Recovery and provide access to the Site to recover the Products as controlled by Section 1.7 above. You are responsible for making sure that You have copies of all Customer Content You require prior to the date of any termination in accordance with Section 1.7 above.

**B. Reserved.**

**4.3 Essential Use/Intent.** Customer agrees that the acquisition, quantity and use of APEX Subscriptions are deemed to be essential to Customer’s operations and Customer seeks to procure the Equipment with the intent to utilize it for this essential performance during the Schedule term.

**5. Prevention and Mitigation.**

You are responsible for Customer Content and for maintaining an IT architecture, as well as processes, enabling You to prevent and mitigate damages in line with the criticality of the Customer Content for Your business and its data protection requirements, including a business recovery plan. You will: (a) provide for a backup process in accordance with industry standards including but not limited to backup relevant data before Reseller or Dell perform any remedial, upgrade or other works on the Products or Your IT systems; (b) monitor the availability and performance of Your IT environment, including the Products; and (c) promptly react to messages and alerts received from Dell or through notification features of the Products and promptly report any issue You identify to Reseller.

**6. Reserved.**

**7. Disclosure of End User Agreement.** You agree Reseller may disclose the Contract to Dell and Dell’s Affiliates.

**8. Definitions.**

**8.1 Reserved.**

**8.2 “APEX End User Subscription Form (Indirect)” or “End User Subscription Form”** means the form listing the Products and Services included in the Subscription and this APEX-Subscriptions

Agreement.

- 8.3 “Asset Recovery”** of a Product means Reseller or Dell taking possession of the Product.
- 8.4 “Billing Period”** means the period of time identified in an Order for which Reseller will invoice You for the Subscription.
- 8.5 “Colocation Site”** means, where applicable, a third-party Site.
- 8.6 “Customer Content”** means data (including but not limited to all text, sound, video, and image files), software (including machine images), and other information You or Your end users store, use or make available to Reseller or Dell through use of the Subscription. As between Customer and Dell, Customer Content is Customer’s Confidential Information, as controlled by Section 11 of the CTS (“Confidentiality”). As between Customer and Reseller, Customer Data is similarly Customer’s Confidential Information under the Contract. Customer Content does not include System Data relating to Your use of the Products and which is described in Section 2.3 (“Telemetry Notice”).
- 8.7 “Dell”** is the Dell Technologies entity which enters into a resale agreement with Reseller and which is the Original Equipment Manufacturer (OEM) of the APEX Subscriptions offer.
- 8.8 “Fee”** means the fees invoiced by Reseller for the Monthly Commitment and the Reserve Usage in each Billing Period during a Subscription Term, up to the maximum amount authorized in the Order. For the avoidance of doubt, in no circumstance shall the total Fees for an Order exceed the total amount authorized in the Order. Any additional fees shall be subject to prior internal State of Illinois written approvals and the requirements and limitations of applicable laws and regulations, including but not limited to the Illinois Procurement Code (30 ILCS 500) and the Illinois Criminal Code (720 ILCS 5/33E-9).
- 8.9 “Measuring Equipment”** means the equipment, software and programming needed for Dell to track usage levels and perform Support Services.
- 8.10 “Monthly Commitment”** means the minimum amount of usage Customer commits to each month as specified in an Order regardless of the actual usage.
- 8.11 Reserved.**
- 8.12 “Professional Services”** are consulting, implementation and any other services that are not Services.
- 8.13 “Reserve Usage”** means the amount of Your flexible consumption usage above the Monthly Commitment.
- 8.14 “Services”** are Dell’s standard service offerings for maintenance and support of Products (“Support Services”) and deployment services (“Deployment Services”).
- 8.15 “Site”** means the location of the Product installation as identified on an Order and the End User Subscription Form.
- 8.16 “Subscription”** means the use of a Product on a flexible consumption basis as measured by the description and metrics from Your Reseller and this APEX-Subscriptions Agreement.
- 8.17 “Subscription Term”** means the time period identified on an Order and the End User Subscription Form for use of the Products, and any extension(s) thereto. The Subscription Term commences on the first day of the month following the date the Products have been installed at the Site, or, if End User delays the installation process or if End User’s Site is not prepared for the installation of the Products, the first day of the second month following the Product’s arrival at the Site.
- 8.18 “Third Party Products”** means hardware, software, products, or services that are not “Dell” or “Dell EMC” branded.
- 8.19 “United States Federal Government End User(s)”** means any department, agency, division or office of the United States federal government.
- 8.20 “U.S. Public End User(s)”** means either (a) a United States Federal Government End User or (b) any U.S. state or local government (i) department, agency, division, or office, (ii) public or higher education institution, or (iii) healthcare entity.

**Exhibit E:**

**Dell Privacy Statement—United States**

Posted at <https://www.dell.com/learn/us/en/uscorp1/policies-privacy>,  
(which shall not impose any legal obligations on the State).