# PARTICIPATING ADDENDUM
# NASPO ValuePoint COOPERATIVE PURCHASING PROGRAM
# Online Auction Services
# Administered by the State of New Mexico (hereinafter “Lead State”)

# NASPO MASTER AGREEMENT
# Master Agreement No: 20-00000-22-00051AB
# Liquidity Services Operations LLC dba GovDeals
# (hereinafter “Contractor”)
# And
# Commonwealth of Kentucky
# (hereinafter “Participating State”)
# MA 758 2300000585

This Participating Addendum Commonwealth Master Agreement (“PA” or “Participating Addendum”) is entered into, by and between the Commonwealth of Kentucky (“Participating Entity” or “Customer”) and Liquidity Services Operations LLC dba GovDeals (“Contractor” or “Vendor” or “GovDeals”).

## Scope and Participation:

1. Scope: GovDeals (“Contractor”) and the State of New Mexico, for itself and on behalf of the NASPO ValuePoint (“NASPO ValuePoint” and/or “Customer”), have entered into a NASPO Master Agreement #20-00000-22-00051AB with an effective date of September 02, 2022, which together with any and all amendments and/or addenda thereto constitute the "Master Agreement".

   This Participating Addendum applies to the use of awarded categories:

   1. Tier 1: Online Auction System
   2. Tier 2: Website and Accounting Operation

Any scope exclusions specified herein apply only to this Participating Addendum and shall not amend or affect other participating addendums or the NASPO Master Agreement itself.

2. Participation: The Commonwealth hereby designates **All State Agencies**, political subdivisions, and authorized non-profits located in the Participating State as authorized Participating Entity(ies) under this Participating Addendum.

3. Term: The term of this Participating Addendum shall begin on March 01, 2023 through September 01, 2024, with annual renewal options not to exceed the final NASPO expiration date of September 01, 2032.

4. Primary Contacts: The following (or their named successors) are the primary contact individuals for this Participating Addendum:

**CONTRACTOR:**

| | |
|---|---|
| Name: | Rebecca Murphy |
| Address: | 100 Capitol Commerce Blvd., Suite 110, Montgomery, AL 36117 |
| Telephone: | 980-254-8908 |
| Email: | rmurphy@govdeals.com |

**PARTICIPATING ENTITY:**

| | |
|---|---|
| Name: | Holly McDonald |
| Address: | 200 Mero St. 5th Floor, Frankfort, KY 40622 |
| Telephone: | 502-564-6523 |
| Email: | Holly.McDonald@ky.gov |

## Participating Entity Modifications and Additions to the Master Agreement

Any limitations, modifications, or additions specified herein apply only to the agreement and relationship between Participating Entity and Contractor and shall not amend or affect other participating addendums or the Master Agreement itself.

☒ This Participating Addendum incorporates all terms and conditions of the Master Agreement as applied to the Participating Entity and Contractor, **subject to the following limitations, modifications, and additions:**

Exhibit A – LSO GovDeals – IT Security and Disaster Recovery and Exhibit B – IT Compliance and Standards are incorporated, hereby within, into the terms and conditions of this Agreement.

**Governing Law:** This Participating Addendum shall be governed and construed in accordance with the laws of the Commonwealth of Kentucky.

The Participating State is agreeing to the terms of the NASPO Master Agreement No: 20-00000-22-00051AB only to the extent the terms are not in conflict with applicable law.

**Commonwealth Office of Technology (COT) Requirements, if applicable:**

30.1 **Commonwealth Information Technology Policies and Standards**

A. The vendor and any subcontractors shall be required to adhere to applicable Commonwealth policies and standards.

B. The Commonwealth posts changes to COT Standards and Policies on its Commonwealth Office of Technology - Home - Commonwealth Office of Technology (Kentucky) website. Vendors and subcontractors shall ensure their solution(s) shall work in concert with all posted changes. Vendors or subcontractors that cannot comply with changes must, within thirty (30) days of the posted change, request written relief with the justification for such relief. The Commonwealth may 1) deny the request, 2) approve an exception to the policy / standard, or 3) consider scope changes to the contract to accommodate required changes. Vendors or subcontractors that do not provide the response within the thirty (30) day period shall be required to comply within ninety (90) days of the change.

30.2 **Compliance with Kentucky Information Technology Standards (KITS)**

A. The Kentucky Information Technology Standards (KITS) reflect a set of principles for information, technology, applications, and organization. These standards provide guidelines, policies, directional statements and sets of standards for information technology. It defines, for the Commonwealth, functional and information needs so that technology choices can be made based on business objectives and service delivery. The vendor shall stay knowledgeable and shall provide a solution that works in concert with these standards for all related work resulting from this Contract.
https://technology.ky.gov/about-the-agency/Pages/kits.aspx

B. The vendor and any subcontractors may be required to submit a technology roadmap for any offered solution. Additional roadmaps will be submitted upon request of the Commonwealth. The roadmap shall include, but is not limited to, planned, scheduled and projected product lifecycle dates and historical release/patch or maintenance dates for the technology. In addition, any guidance on projected release/revision/patch/maintenance schedules would be preferred.

30.3 **Compliance with Commonwealth Security Standards**

The software deployment and all vendor services shall abide by privacy and security standards as outlined in the Commonwealth's Enterprise Information Technology Policies.

**Enterprise Security Policies**
https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx

**Enterprise IT Policies**
https://technology.ky.gov/policies-and-procedures/Pages/policies.aspx

30.4 **Compliance with Industry Accepted Reporting Standards Based on Trust Service Principles and Criteria**

The vendor must employ comprehensive risk and threat management controls based on defined industry standards for service organizations such as ISO AICPA TSP section 100, Trust Services Principles and Criteria. The vendor must annually assert compliance and engage a third party certification registrar to examine such assertions and controls to provide a Report, such as ISO 9000, ISO 14001, AT101 SOC 2 type 2, on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy, which contains an opinion on whether the operating controls effectively support the assertions. All such reports, including publicly available reports (i.e. AT 101 SOC 3) shall be made available to the Commonwealth for review.

30.5 **System Vulnerability and Security Assessments**

The Commonwealth reserves the right to conduct, in collaboration with the vendor, non-invasive vulnerability and security assessments of the software and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of these assessments, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls that will reduce risk to an acceptable and agreed upon level. An accredited third party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

30.6 **Privacy Assessments**

The Commonwealth reserves the right to conduct Privacy assessments of the collection, use, maintenance and sharing of Commonwealth data by any vendor services, software, and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of this assessment, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls or privacy practices that will reduce risk to an acceptable and agreed upon level. An accredited third-party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

30.7 **Privacy, Confidentiality and Ownership of Information**

The Commonwealth is the designated owner of all Commonwealth data and shall approve all access to that data. The Vendor shall not have ownership of Commonwealth data at any time. The vendor shall not profit from or share Commonwealth data. The Vendor shall be in compliance with privacy policies established by governmental agencies or by state or federal law. Privacy notice statements may be developed and amended from time to time by the Commonwealth and will be appropriately displayed on the Commonwealth portal (Ky.gov). The Vendor should provide sufficient security to protect the Commonwealth and COT data in network transit, storage, and cache. **All Commonwealth data, including backups and archives, must be maintained at all times within the contiguous United States. All Commonwealth data, classified as sensitive or higher, as defined in Enterprise Standards, must be encrypted in-transit from Contractor's network and at rest while stored on Contractor's laptops or other portable media devices.**

30.8 **EU GDPR Compliance**

The Commonwealth of Kentucky requires all vendor contracts to comply to the extent applicable with the European Union's General Data Privacy Regulation [Regulation (EU) 2016/679] (the "GDPR") when the Commonwealth is a "controller" or "processor" of "personal data" from an individual "data subject" located in the European Union, as those terms are defined in the GDPR. The Contractor acknowledges and agrees that it is acting as a "processor" of "personal data" for the Commonwealth under this Agreement and that all applicable requirements of the GDPR are incorporated by reference as material terms of this Agreement. The Contractor represents and warrants that (1) it is aware of and understands its compliance obligations as a "processor" under GDPR; (2) it has adopted a GDPR compliant data privacy compliance policy/program, a summary of which has been provided to the Commonwealth; (3) it will process "personal data" only in accordance with the Commonwealth's instructions; and (4) with regard to its obligations under this Agreement, it shall comply with all applicable requirements of the GDPR. Additionally, the Contractor may be found liable to the Commonwealth for damages arising from any violation of applicable requirements of GDPR by the Contractor in its performance of the services hereunder, subject to Section 40.31, entitled Contractor's Limitation of Liability.

30.9 **X-as-a-Service Technical Definitions**

Refer to NIST 800-145

## 30.10 Data Quality

Vendors shall provide proposed levels of data quality per the following dimensions.

Data Quality is the degree to which data is valid, accurate, complete, unique, timely, consistent with all requirements and business rules, and relevant for a given use. The vendor shall provide data quality definitions and metrics for any data elements. Data has to be of the appropriate quality to address the needs of the Commonwealth of Kentucky. The following dimensions can be used to assess data quality:

- Validity – The data values are in an acceptable format.
- Accuracy – The data attribute is accurate.
- Completeness – There are no null values in a data field.
- Uniqueness – There are no duplicate values in a data field.
- Timeliness – The data attribute represents information that is not out-of-date.
- Consistency – The data attribute is consistent with a business rule that may be based on that attribute itself, or on multiple attributes.
- Adherence to business rules – The data attribute or a combination of data attributes adheres to specified business rules.

## 30.11 Metadata Requirement

The awarded Vendor shall provide a glossary for all business terms used in this solution.

## 30.12 System Security Compliance Requirements

A. Session Security Lock

Vendor shall configure:

1. The system to initiate a session lock after a maximum of fifteen (15) minutes of inactivity.
2. The system session will remain locked until the user re-established identification and authentication procedures.

B. Session Pattern-Hiding Displays

Vendor shall configure system to conceal information previously visible on the display with a publicly viewable image or blank screen. When a session locks or times out, the system shall obfuscate or blank out the displayed screen and data at the time of the session lock as to not risk exposure after the session lock.

C. Session Termination

Vendor shall configure system to terminate a user session automatically after defined conditions trigger events requiring session disconnect. Conditions or trigger events requiring automatic session termination include, but are not limited to:

1. Agency-defined periods of user inactivity,

2. Targeted responses to certain types of incidents, or
3. Time-of-day restrictions on information system use.

30.13 **Software Development**

Source code for software developed or modified by the vendor specifically for the Commonwealth shall become property of the Commonwealth. This is not meant to include minor modifications to the vendor software to configure the software for Commonwealth use. This is meant to include software written to add functionality to the vendor product specifically to meet the requirements of the Commonwealth where the Commonwealth bears the entire cost of creating that functionality.

30.14 **License Agreements**

Software provided by the vendor to the Commonwealth should contain a provision for perpetual licensing with all upgrade options. License agreements should also contain a provision for the Commonwealth to maintain a version of the software in escrow in the event the vendor is unable to continue business for financial or other business reasons.

Any escrow agreement shall be negotiated by all parties.

Any third-party software licenses and cloud resources necessary for the proposed solution may be procured via the Commonwealth's existing contracts.

30.15 **Software Version Requirements**

All commercially supported and Commonwealth approved software components such as Operating system (OS), Database software, Application software, Web Server software, Middle Tier software, and other ancillary software must be kept current. In the event that a patch interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution in to compliance to allow this patch to be applied in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

The Vendors shall keep software in compliance with industry standards to support third party products such as Java, Microsoft Edge, Mozilla Firefox, etc. at latest supported version, release, and patch levels, when such dependencies exist. In the event that a third party dependency interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution into compliance to allow this third party dependency to be updated in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

30.16 **No Surreptitious Code Warranty**

The contractor represents and warrants that no copy of licensed Software provided to the Commonwealth contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this contract as the "No Surreptitious Code Warranty".

As used in this contract, "Self-Help Code" means any back door, time bomb, drop-dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access) for purposes of maintenance or technical support.

As used in this Contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code.

In addition, Contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the Commonwealth.

The vendor shall defend the Commonwealth against any claim, and indemnify the Commonwealth against any loss or expense arising out of any breach of the No Surreptitious Code Warranty.

30.17 **Network Connection Requirements**

A. Vendor shall work with COT to establish any network connections. If a secure site-to-site connection is required, the vendor shall employ a secure site-to-site connection procured by the Agency from COT.

B. Vendor shall notify COT of network bandwidth requirements and if caching is required for implementation vendor shall resolve caching requirements, in coordination with COT.

C. Vendor shall, at COT's discretion, provide appropriate access to enable the Commonwealth to perform additional security measures, such as decryption of the network traffic if required for inspection. If the proposed solution does not have the ability to meet this requirement, the vendor must provide an alternative such as audit reporting of this function.

D. Vendor shall provide notifications to the Commonwealth Service Desk for unplanned outages within 5 minutes.

E. Vendor shall notify COT Change Management, through the Commonwealth Services Desk, a minimum of two (2) business days prior to any planned outage.

F. Vendor, in conjunction with the agency, shall provide a Business Impact Assessment (BIA) to appropriately classify all data before production/go-live.

G. Vendor shall include a Web Application Firewall when application houses any data classified as sensitive or higher as defined in KITS standards.

H. Vendor shall provide Recovery Time Objective (RTO) and Recovery Point Objective (RPO) services. Vendor shall provide those services to achieve those SLAs.

30.18 **OS Requirements**

A. Non-On Prem Solutions
   1. No Commonwealth data shall be co-mingled with another entity, without the prior approval of the Commonwealth.
   2. Vendor shall provide a solution to move data to the Commonwealth, if required by the Commonwealth.
      a. At the end of the contract, the Vendor shall provide all agency data in a useable standard data format (such as asci, csv, etc.) that can be converted to a subsequent system. The Vendor shall cooperate to this end with the Agency and/or a Vendor of the agency's choice, in a timely and efficient manner.
      b. Vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the vendor of the agency's choice, in a timely and efficient manner.
      c. Vendor shall provide address the destruction of Commonwealth data as defined in CIO-092 and provide a certification of the complete and permanent deletion the Commonwealth data.

B. Infrastructure As A Service
   1. Vendor shall work with the Agency and COT to establish all administrative personnel engagements.
   2. All virtual environments must run on VMC (VMWare Cloud) with OS version compliant with KITS, unless explicitly approved by COT.
   3. VMC shall provide an enterprise class malicious code protective solution that is currently supported by the vendor and up to date

4. Vendor shall meet certification requirements for classification of data being stored.
5. Vendor shall, at COT's request, provide appropriate access to enable the Commonwealth to perform additional security measures in compliance with Commonwealth Enterprise Policies, Standards, and/or any Federal or State requirements.
6. Vendor shall provide an Exit Strategy, to move all data to the Commonwealth Data Center, if required by the Commonwealth.
   a. At the end of the contract, the Vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The Vendor shall cooperate to this end with the Vendor of the agency's choice, in a timely and efficient manner.
   b. Vendor shall provide certification of the complete and permanent deletion of Commonwealth data and backups from all vendor storage.

30.19 **Project Governance**

Vendor shall work with the Agency and appropriate COT offices, when needed, in the cases of data governance, security aspects, hosting, integration, etc., provided that such work does not expand the scope of the services as described in Section 50 absent a corresponding change order agreed to by the parties reflecting such expansion.

30.20 **Monitoring Requirements for On Premise and Cloud (SaaS)**

Vendor shall work with the Agency and COT to establish a monitoring solution. Vendors shall provide a view into their environment either by providing a COT approved comprehensive dashboard or allow COT to install their KITS compliant monitoring solution; to include but not limited to performance and availability.

30.21 **Application and Service Requirements**

A. Current Enterprise Applications and Services
   1. COT provides a number of Enterprise Shared Services to State agencies. Vendor shall use published IT Applications and Services provided on KITS for: Enterprise Service Bus, Enterprise Content Management, Data Warehousing, Data Analytics and Reporting, Business Intelligence, Web Services, GIS, unless explicitly approved by COT.
   2. Vendor provided dedicated application components (i.e., Application Servers, Databases, etc.) shall comply with KITS or if the technology is not included in KITS, the technology must be accepted by the Commonwealth for inclusion in KITS or granted a written exception to KITS according to COT Information Technology Standards Policy currently CIO-051.
   3. Vendor applications must describe in detail all available features and functionality accessible via APIs.
   4. All business applications must support the ability to use modern authentication for authentication and authorization. Modern authentication

technologies would include SAML 2.0, WSFED, OAuth, or OpenID Connect.

B. Vendor shall comply with Commonwealth of Kentucky fingerprint requirements for PII/FTI/HIPAA data systems hosted outside Central Data Center. The current standard is included in the IRS publication 1075 which can be found here: https://www.irs.gov/pub/irs-pdf/p1075.pdf

30.22 **Project Management Requirements**

The COT Division of Governance and Strategy (COT-DGS) is responsible for overseeing large and complex technology projects throughout the Commonwealth. The vendor shall adhere to Project Management standards and reporting requirements established by COT-DGS, which are posted at https://technology.ky.gov/services-and-support/Pages/About-the-Project-Management-Branch.aspx. These include, but are not limited to, having a documented project schedule, risk management, issue management and reporting project status to the CIO monthly in the format defined by COT-DGS. In addition to the project management standards required by COT-DGS, agency specific requirements may be defined in this Contract.

30.23 **Applicable Security Control Framework Compliance**

The vendor must have an awareness and understanding of the NIST Special Publication 800-53 Security Control Framework and employ safeguards that meet or exceed the moderate level controls as defined within the standard. The respondent must provide sufficient safeguards to provide reasonable protections around the Commonwealth's data to ensure that the confidentiality, integrity, and availability is maintained at an appropriate level. These include but are not limited to:

- *Access Control*
  The vendor must employ policy and process that provide for stringent control to limit physical and logical access to systems that house Commonwealth data, on a need to know basis, provide clear separation of duties, and adheres to least privilege principles.
- *Awareness and Training*
  The vendor must provide the appropriate role specific training for staff to ensure that there is awareness and understanding of roles and responsibilities as they relate to the protections around the Commonwealth's data.
- *Audit and Accountability*
  There must be sufficient auditing capability to ensure that actions are tracked and there is individual accountability for all actions taken by vendor staff.
- *Configuration Management*
  The vendor must work within established baselines that provide minimal functionality needed to ensure service delivery without exposing unnecessary risk. The vendor must also employ structured change control processes that provide a level of coordination with the client agreed upon in a Service Level Agreement (SLA).

- *Contingency Planning*
  The vendor must employ contingent planning policy and procedures that ensure service delivery based on agreed SLA levels while maintaining all Commonwealth data within the continental Unites States.
- *Identification and Authorization*
  The vendor must employ appropriate identity and access management policies and procedures to ensure that access is appropriately authorized and managed at a level to ensure that access is provisioned and de-provisioned in a timely and efficient manner.
- *Incident Response*
  The vendor must employ policy and procedures to ensure that an appropriate response to all identified security incidents are addressed in a timely manner and are reported to the appropriate parties in an agreed upon SLA timeframe. The vendor must also ensure that all staff are sufficient trained to ensure that they can identify situations that are classified as security incidents.
- *Maintenance*
  The vendor must employ policy and procedures that ensure that all maintenance activities are conducted only by authorized maintenance staff leveraging only authorized maintenance tools.
- *Media Protection*
  The vendor must employ policy and procedure to ensure that sufficient protections exist to protect Commonwealth data on all storage media throughout the media lifecycle and maintain documentation from media creation through destruction.
- *Physical and Environmental Controls*
  The vendor must employ physical and environmental policies and procedures that ensure that the service and delivery infrastructure are located in a physically secure and environmentally protected environment to ensure the confidentiality, integrity, and availability of Commonwealth data.
- *Personnel Security*
  The vendor must employ policies and procedures to ensure that all staff that have access to systems that house, transmit, or process Commonwealth data have been appropriately vetted and have been through a background check at the time of hire and periodically thereafter.
- *System and Communications Protections*
  The vendor must employ physical and logical protection that protect system communications and communication media from unauthorized access and to ensure adequate physical protections from damage.

1. Lease Agreements: ***Reserved****.*

2. Subcontractors: All contractors, dealers, and resellers authorized to provide sales and service support in Participating Entity's state, as shown on Contractor's NASPO ValuePoint-specific webpage, may provide sales and service support to users of this Participating Addendum. Participation of Contractor's contractors, dealers, and resellers will be in accordance with the terms and conditions set forth in the Master Agreement.

3. Orders: Any order placed by Participating Entity or a Purchasing Entity for a product or service offered through this Participating Addendum shall be deemed to be a sale under, and subject to the pricing and other terms and conditions of, the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to the order.

4. Pricing: The State Agencies receive one-hundred percent (100%) of all proceeds and/or dividends from items sold on the online auction system at no cost to the Commonwealth.

IN WITNESS WHEREOF, the Parties have executed this Participating Addendum.

| **PARTICIPATING ENTITY** | **CONTRACTOR** |
|---|---|
| Commonwealth of Kentucky<br>Finance Facilities | Liquidity Services Operations LLC dba GovDeals |
| Signature:<br>DocuSigned by:<br>Sam Ruth<br>F8175574F0A046A... | Signature:<br>DocuSigned by:<br>Michael Price<br>CCB19588953C4C0... |
| Name:<br>Sam Ruth | Name:<br>Michael Price |
| Title:<br>Commissioner | Title:<br>Vice President, Revenue |
| Date:<br>2/22/2023 | Date:<br>2/22/2023 |
| Commonwealth of Kentucky<br>Office of Procurement Services (OPS) | |
| Signature:<br>DocuSigned by:<br>Kathy Robinson<br>12A54A21C03A4F2... | |
| Name: Kathy Robinson | |
| Title: Executive Director | |
| Date:<br>2/23/2023 | |

*ATTACHMENTS:*

*Exhibit A – LSO GoveDeals – IT Security and Disaster Recovery*

*Exhibit B – LSO GovDeals – IT Compliance and Standards*

For questions regarding NASPO ValuePoint Participating Addendums, please contact the Cooperative Contract Coordinator team at info@naspovaluepoint.org.

Fully executed NASPO ValuePoint Participating Addendums must be submitted via email in PDF format to pa@naspovaluepoint.org.

Exhibit A

GovDeals®
A Liquidity Services Marketplace

**Liquidity Services Operations LLC (o/a GovDeals)**
100 Capitol Commerce Blvd., Suite 110
Montgomery, AL 36117
1-800-613-0156 | www.GovDeals.com

**NASPO ValuePoint Information**
**Requested by Commonwealth of Kentucky**

1. Page 23, Item 11 of the agreement states:

11. Contractor shall provide all security systems, anti-virus and firewalls capable of preventing the hacking of any auction information from the auction servers, capable of preventing the assimilation or distribution of viruses and other programs and capable of preventing any bidder from learning the identity of any other bidder. Offeror must submit a written narrative explaining how the Offeror shall meet this requirement. The information supplied in this narrative will be scored.

Can you provide me with the written narrative Liquidity Services Operations, LLC, dba GovDeals submitted in response to this requirement?

GovDeals will provide all security systems, anti-virus and firewalls capable of preventing the hacking of any auction information from the auction servers, capable of preventing the assimilation or distribution of viruses and other programs and capable of preventing any bidder from learning the identity of any other bidder. GovDeals employs many systems to ensure that its operations are secure from hacking or other disruption.

Following is the short list of the core applications and services we use for endpoint management:

- Microsoft Defender – this is both an anti-virus and EDR (endpoint detection and response) and is installed across our endpoints.
- Microsoft Sentinel – this is centralized log management and alerting system (SEIM) that receives the input signals from all our endpoints (via Defender) as well as our Azure Active Directory. With this information it allows us to detect and respond to threats across the enterprise, in real time.
- Microsoft Endpoint Manager (SCCM + InTune) – we currently use two different but related Microsoft products for device patch management. These are:
    - System Center Configuration Manager – used for patch management of our 'on premise' hardware
    - InTune - used for managing the configuration and patching of our warehouse tablets and cloud-only joined devices
- Additionally, we have a variety of tools from Palo Alto, Cisco, and Qualys that provide perimeter defense functions, URL scanning, as well as active vulnerability scanning of the environment.

2. Page 23, Item 12 of the agreement states:

12. Contractor shall provide contingency plans to backup information and recover information. The Contractor shall have a disaster recovery plan that covers internet failure, electricity failure or systems failures.

Can you provide me with a copy of the contingency plans or Disaster Recovery Plan Liquidity Services Operations LLC, dba GovDeals submitted in response to this requirement?

See attachment.

LIQUIDITY SERVICES

*A Better Future for Surplus*

# GovDeals Disaster Recovery Plan Description

The GovDeals disaster recovery plan begins with the underlying application architecture. The website's infrastructure is designed for scale, availability, and survival by employing multiple resiliency techniques, including load balanced servers, data replication, and geographic redundancy. Combined these techniques allow GovDeals to meet our customers' availability needs.

The infrastructure is hosted on the Microsoft Azure cloud platform, which supports our redundancy and scalability goals. The site is load-balanced across multiple servers, providing the ability to both scale the application as well as withstand the loss of servers without incurring a disruption. The underlying database operates in a high availability, multi-node cluster configuration that is fully replicated between database nodes in a multi-region configuration. All critical auction and customer data are replicated between nodes in multiple, geographically disbursed, datacenters.

## Failure Scenarios

| **Application Tier** | **Type of Failure** | **Recovery Mechanism** |
|---|---|---|
| Web Servers | Individual server failure | Pull from load balanced cluster and replace |
| Application Servers | Individual server failure | Pull from load balanced cluster and replace |
| Database Server | DB failure, primary node | Fail over to secondary node, same region |
| Database Server | DB failure, secondary node | Rebuild and join replication cluster |
| Azure Region | Complete region failure | Move primary DB node responsibility to backup region, bring cold webservers online |
| Database Records | Critical failure | Recover from disconnected backup |

GovDeals utilizes multiple internal and external site monitoring systems to ensure appropriate responses to any warnings, critical issues, or other matters that need immediate attention 24 hours a day, 7 days a week, and 365 days a year.

Exhibit B

6931 Arlington Road, Suite 200
Bethesda, MD 20814 United States
T: (202) 467 6868
F: (202) 467 2345
www.LiquidityServices.com

**Commonwealth of Kentucky**

In response to your request '***How does GovDeals assess the compliance of their environment and to what standard?***'.

Please see below our attestation of compliance (AOC) that the following activities are being undertaken. We have provided as much detail as possible for each of these activities, including service provider, frequency, and products used.

On the basis that, Liquidity Services (Trading as GovDeals) does not provide any documentation to external parties that could prejudice our overall security posture, thereby increasing our own risk profile.

## Risk Assessments

Liquidity Services performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and risks from these threats are formally assessed.

The primary areas are:

- Identification
- Protection
- Detection
- Response
- Recovery

## ICFR SOX Compliance Review

Additionally, and as an integral part of our ongoing commitment to the Sarbanes Oxley act as a publicly held American company. Our IT General Controls are subject to validated third party testing at various points over the course of the financial year. These control audits are conducted with both our internal (Grant Thornton), and external (Ernst & Young) audit partners. These procedures include a risk assessment at both the system (ITGC), and the business process level.

Providers: Grant Thornton, LLP & Deloitte, LLP
Services: Internal & External Audit Partners
Frequency: Annually

**PCI DSS Compliance**

Liquidity Services maintains PCI DSS compliance across our marketplace entities.

Liquidity Services utilizes a Tier 1 payments provider (Braintree Payments – A PayPal company) to facilitate the tokenization of all customer card data. As a company we do not store or process credit card information within our systems.

**Dynamic Vulnerability Analysis**

Provider: Qualys, Inc
Product: VMDR
Frequency: Weekly Scans

Vulnerability Management, Detection and Response (VMDR) enables Liquidity Services to discover, assess, prioritize, and patch critical vulnerabilities and misconfigurations in real time and across our global hybrid-IT landscape all in one solution.
This helps reduce our total time to remediate and secure our environment faster.
It helps Liquidity Services obtain continuous vulnerability assessments with cloud agents, network level visibility using network scanners and multiple types of sensors' and leverages artificial intelligence to instantly assess and prioritize threats based on relevant context.

**Penetration Testing**

Liquidity Services have penetration tests performed by qualified external service providers at least annually. The penetration tests are carried out according to documented test methods and include the infrastructure components, and web applications defined to be critical to the secure operation of the services we provide.

Provider: Breachlock, Inc.
Service: Penetration Testing

Regards,

Matthew Saxton
Director, IT Security & Compliance
Date: 03 Feb 2023