SECOND AMENDMENT
TO
MASTER AGREEMENT
BETWEEN
THE STATE OF CONNECTICUT, DEPARTMENT OF ADMINISTRATIVE SERVICES
AND
GUIDESOFT, INC. DBA KNOWLEDGE SERVICES
FOR
IT MANAGED SERVICE PROVIDERS

This Second Amendment (the "Second Amendment") is made between the GuideSoft, Inc. dba Knowledge Services (the "Contractor") and the State of Connecticut, Department of Administrative Services ("DAS") in accordance with Sections 4a-2(2), 4a-51, 4a-57, and 4a-59 of the Connecticut General Statutes.

WHEREAS, DAS and the Contractor entered into a Master Agreement Number 22PSX0086AB dated November 1, 2023 for the provision of Managed Service Provider ("MSP") services and an operational Vendor Management System ("VMS") for information technology ("IT") staffing resources, payroll staffing, and staffing support related to Contingent Workers in the IT industry, as amended on September 17, 2024 (the "Master Agreement"); and

WHEREAS DAS and Contractor desire to amend the Master Agreement with this Second Amendment to update Exhibit A, Description of Deliverables, extend the Master Agreement Term, and otherwise to update the Master Agreement to comply with current State of Connecticut contract requirements.

NOW, THEREFORE, DAS and Contractor agree to amend the Master Agreement as follows:

A. The following new subsection G: "Federal Tax Information ("FTI") Security Requirements" is added to Section II, Additional Terms and Conditions, in Exhibit A, Description of Deliverables:

    1. "In Performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by its officers and employees with the following requirements:
        i. Access to FTI and Background Checks. All work will be Performed under the supervision of the Contractor or the Contractor's responsible employees. The Contractor shall ensure that only Contractor's officers and personnel who have passed background check requirements defined in the Internal Revenue Service ("IRS") Publication 1075, are granted access to FTI. A current list of such authorized individuals shall be maintained by the Contractor and made available to the State, the Exchange, and the IRS upon request.
        ii. Use and Disclosure Restrictions. FTI, in any format (electronic or hardcopy), shall be used solely for the Performance of services under this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the Performance of this Contract. Inspection or disclosure of FTI to anyone other than the Contractor or the Contractor's officers or employees authorized is prohibited.
        iii. Storage, Handling, and Destruction.
            a) FTI will be accounted for upon receipt and properly stored before, during, and after processing.

b) Any related output and products require the same level of protection as required for the source material.
c) The Contractor shall certify that FTI processed during the Performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed.
d) If immediate purging of physical and electronic data storage is not possible, the Contractor shall certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
e) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the Exchange by the Contractor. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the Exchange with a statement containing the date of destruction, description of material destroyed, and the destruction method.

iv. System Security Controls. All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

v. Subcontracting Restrictions.
a) No work involving FTI furnished under this Contract will be subcontracted without the prior written approval of the IRS.
b) The Contractor shall ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI. To the extent this Contract's terms, conditions, duties, and obligations relate to Services Performed with FTI, the Contractor must treat the subcontractor as the Exchange would treat the Contractor. The Contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the Exchange under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the Exchange under this Contract.
c) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the Contractor is bound and obligated to the Exchange under this Contract. For purposes of this Contract, the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI. The Exchange will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

vi. Criminal and Civil Sanctions.
a) Each officer or employee of the Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or

employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as five thousand dollars ($5,000) or imprisonment for as long as five (5) years, or both, together with the costs of prosecution.

b) Each officer or employee of the Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access or inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as one thousand dollars ($1,000) or imprisonment for as long as one (1) year, or both, together with the costs of prosecution.

c) Each officer or employee of the Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of one thousand dollars ($1,000) for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access or inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by Internal Review Code ("IRC") sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

d) Contractor shall inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his or her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than five thousand dollars ($5,000).

vii. Certification Requirements. Granting the Contractor access to FTI must be preceded by certifying that each officer or employee understands the Exchange's security policy and procedures for safeguarding FTI. The Contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the Exchange's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the Exchange's files for review. As part of the certification and at least annually afterwards, the Contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431. The training on the Exchange's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For

the initial certification and the annual recertifications, the Contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

viii. Inspection. The IRS and the Exchange, with twenty-four (24) hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of IT assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

B. The Master Agreement Term is extended to October 31, 2029, in accordance with Section 2, Term of Master Agreement; Master Agreement Extension, of the Master Agreement.

C. Section 45, Summary of State Ethics Laws, is deleted in its entirety and the following is substituted in its place:

"45. Summary of State Ethics Laws

Pursuant to the requirements of section 1-101qq of the Connecticut General Statutes (a) the State has provided to the Contractor the summary of State ethics laws developed by the Office of State Ethics pursuant to section 1-81b of the Connecticut General Statutes, which summary is incorporated by reference into and made a part of this Contract as if the summary had been fully set forth in this Contract; (b) the Contractor represents that the chief executive officer or authorized signatory of the Contract and all key employees of such officer or signatory have read and understood the summary and agree to comply with the provisions of state ethics law; (c) prior to entering into a contract with any subcontractors or consultants, the Contractor shall provide the summary to all subcontractors and consultants and each such contract entered into with a subcontractor or consultant on or after July 1, 2021, shall include a representation that each subcontractor or consultant and the key employees of such subcontractor or consultant have read and understood the summary and agree to comply with the provisions of state ethics law; (d) failure to include such representations in such contracts with subcontractors or consultants shall be cause for Termination of the Contract; and (e) each contract with such contractor, subcontractor or consultant shall incorporate such summary by reference as a part of the contract terms."

D. The following is added as a new section 58 to the Master Agreement: "Prohibition on Additional Terms of Use:

a. The Contractor shall not require, as a condition of access to or use of any Deliverable under this Contract, that the State or its authorized Users agree to or be bound by any terms of use, service terms, privacy policy, click-through agreement, shrink-wrap agreement, browse-wrap agreement, or any other form of supplemental, unilateral or online terms that are not already incorporated into this Contract (collectively, "Supplemental Terms").

b. Any Supplemental Terms, whether presented before, during, or after delivery or access to or use of the Deliverables, are rejected and shall have no force or effect, regardless of any action or inaction of a User (including, but not limited to, clicking "I agree," opening a hyperlink, accessing a website, or continuing use of a service).

c. The Contractor may require the State or its Users to accept limitations on use only if those limitations are specifically set forth in, and are consistent with, all other terms of this Contract. No limitation on use shall be enforceable unless expressly previously agreed to in writing by the State.

d. Imposing, or any attempt to impose, Supplemental Terms on the State or its Users constitutes a material breach of this Contract. This provision is governed by Connecticut law and does not limit any right or remedy available to the State under Connecticut law or this Contract."

This Second Amendment is effective on the date of the last party to execute below.

All other terms and conditions not otherwise affected by this Second Amendment remain in full force and effect.

The parties are executing this Second Amendment on the date below their respective signatures.

GUIDESOFT, INC. DBA KNOWLEDGE SERVICES	STATE OF CONNECTICUT Department of Administrative Services
NASPO ValuePoint is in receipt of the Lead State's duly executed Second Amendment.	
By: _____	By: _____
Name: _____ Print or Type Name	Name: Mark Raymond
Title: _____	Title: Chief Information Officer
Date: 2/2/2026	Date: 2/13/2026