MASTER SERVICES AGREEMENT
FOR SERVICES PROVIDED TO
STATE OF MAINE

This Master Services Agreement (this "Agreement"), dated the day of , 20 (the "Effective Date"), is made by and between GuideSoft, Inc. dba Knowledge Services with an address of 5875 Castle Creek Parkway, Suite 400, Indianapolis, IN 46250, ("Knowledge Services") and , with an address of ("Vendor").

WHEREAS, Knowledge Services has been contracted by the State of Maine ("the State"), who has signed a Participating Addendum to utilize the NASPO ValuePoint Cloud Solutions Contract ("Master Agreement AR 2504"), led by the State of Utah, to be the Managed Service Provider for certain information technology project services ("Services");

WHEREAS, Knowledge Services desires to engage the Vendor to provide certain temporary information technology staffing services ("Services") as described herein to the State;

WHEREAS, Vendor desires to undertake such work;

WHEREAS, the parties mutually desire to set forth the terms and conditions under which such Services shall be provided; and

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Knowledge Services and Vendor agree as follows:

1. **Services.**
   a. Vendor shall provide Services in accordance with the specifications set forth in this Agreement, including all Exhibits attached to this Agreement, and as specifically set forth in the dotStaff™ vendor management system ("VMS"). By executing this Agreement, Vendor represents that it has the requisite expertise to satisfactorily perform the Services as described in this Agreement.
   b. Master Agreement #AR 2504 has been awarded by the State of Utah as Lead State, consisting of the following documentation that is available on NASPO ValuePoint's website at https://www.naspovaluepoint.org/portfolio/cloud-solutions/knowledge-services/. This Agreement incorporates by reference the terms and conditions contained in such documents. Vendor agrees to be bound by the relevant terms found therein, including but not limited to the below. In the event of an inconsistency or conflict between the terms, Master Agreement #18P-200416*130 shall control.
      - Master Agreement #2504; including all relevant solicitation documents; and
      - Master Agreement MA 18P 200416*130 between Knowledge Services and the State of Maine.
   c. This Agreement inures to the benefit of the State, and the State may separately rely upon and enforce the provisions of this Agreement against Vendor. The State does not allow any modifications to this Agreement.
   d. The relationship established by this Agreement is nonexclusive. In the event that Knowledge Services deems it necessary and appropriate, Knowledge Services may obtain Services and Resources other than through Vendor.

2. **License; Ownership of Software.**
   a. Knowledge Services shall administer and manage the process of identifying and acquiring Resources through Vendor using the VMS, in accordance with the terms of this Agreement; provided that the State shall make the final selection of any Resources presented by Vendor.
   b. For the Term (as defined below), Knowledge Services hereby grants to Vendor a non-exclusive, non-transferable, non-assignable worldwide, license to access and use the VMS hosted on the dotStaff™ website, located at www.dotstaff.com, in conjunction with the terms of this Agreement.
   c. The parties hereby acknowledge and agree that (i) all rights, title and interest in and to the VMS and the documentation are, and shall remain, vested solely in the applicable owner.
   d. Knowledge Services maintains information about Vendor and the fulfillment of Services on servers and/or database systems either used or owned by Knowledge Services. This information includes, but is not limited

to, Vendor information, bids, resumes, budget and other information. Knowledge Services shall exercise all reasonable efforts to maintain and preserve the privacy of Vendor. Knowledge Services may, however, disclose Vendor account information in the good faith belief that such action is reasonably necessary to: (1) comply with a legal order, or (2) enforce this Agreement. Vendor is entirely responsible for any and all activities that occur in connection with Vendor accounts and passwords. Vendor agrees to keep its password(s) confidential, and to notify Knowledge Services promptly if Vendor has any reason to believe that the security of a Vendor account has been compromised.

e. Vendor warrants that: (1) it has the authority and the right to enter into this Agreement, to perform Services hereunder, and that its obligations hereunder are not in conflict with any other obligations; (2) its Resources have the proper skill, training and background necessary to accomplish assigned tasks; and (3) all Services will be performed in a competent and professional manner, by qualified personnel and will conform to the requirements hereunder.

f. Knowledge Services makes and Vendor receives **NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

g. Vendor agrees that it is solely responsible for all actions and communications undertaken or transmitted under Vendor account. Knowledge Services assumes no responsibility or liability for any content entered or otherwise transmitted by Vendor, the State, Resources or any other third parties. Knowledge Services assumes no liability for any mistakes, defamation, slander, libel, falsehoods, omissions, obscenity or pornography that Vendor might encounter through the use of this service.

h. Knowledge Services reserves the right, but does not have the obligation, to remove any content or materials that it deems objectionable at any time. Knowledge Services may delete Vendor content and/or terminate Vendor accounts which Knowledge Services believes (1) involve fraudulent or illegal content; (2) are the subject of complaints regarding conduct or performance; or (3) are the subject of a government complaint or investigation. Knowledge Services may periodically delete stored resumes and/or other information if it becomes necessary, or in its own discretion, determines is obsolete.

i. Knowledge Services reserves the right to perform periodic modifications to the VMS including but not limited to customary maintenance, bug fixes, and upgrades, as Knowledge Services deems necessary or desirable. Such modifications do not require prior notification of Vendor, and may involve the temporary interruption of the VMS, for which Knowledge Services expressly disclaims any liability or responsibility. Knowledge Services will, however, make all reasonable efforts not to disrupt Vendor's access to the VMS for an unreasonable period of time.

3. **<u>Rates and Payment Procedures.</u>**

a. Maximum hourly rates will be developed and provided to Vendor, and the link to such rates is provided in Exhibit A, in addition to other applicable rate information. Such rates shall be effective July 1, 2020. These rates represent the maximum or "not to exceed" rates only, and Vendor shall bid on positions competitively through the VMS.

b. The "Posting and Response Process," attached as Exhibit B, defines the general job requisition and resume submittal procedures for Vendor.

c. Vendor shall ensure that its Resources enter time weekly in the VMS, for approval by the State. The State shall receive invoices for approved time from Knowledge Services biweekly (such invoice frequency is subject to change upon notice to Vendor), and shall submit payment to Knowledge Services for such invoices. In the event of Resource conversions, Vendor shall enter all such information in the VMS, and the State shall remit payment to Knowledge Services for such invoices.

d. Knowledge Services shall charge Vendor an MSP Fee in the amount of two point two five percent (2.25%) of each invoice. Effective with time worked as of July 5, 2020, an additional one percent (1%) rebate fee shall payable to the State, for a total fee of three point two five percent (3.25%) Fee ("Fee"). Knowledge Services shall remit payment to Vendor within ten (10) business days of its receipt of payment from the State (excluding national bank holidays and once funds are available), after deducting the Fee. All rates are inclusive of the Fee.

e. Vendor may enter all direct <u>pre-approved</u>, <u>reimbursable</u> expenses into the VMS for payment by the State, but such expenses shall not be subject to the Fee. Expenses may be pre-approved only by the State, and will not

be reimbursable unless indicated on the job posting that such expenses may be reimbursed in accordance with the rules and regulations applicable to the State employee travel.

f. Knowledge Services shall only pay Vendor upon the receipt of payment from the State. In the event that the State withholds payment with respect to a Resource for any reason, Knowledge Services shall have no obligation to pay Vendor unless and until Knowledge Services is first paid by the State. Knowledge Services' sole obligation shall be to exercise commercially reasonable efforts to collect payment from the State. If for any reason the State refuses or fails to make payment to Knowledge Services for Services rendered, Knowledge Services shall not be liable to make payment to the Vendor, and the Vendor shall not be liable to pay the related Fee to Knowledge Services. Vendor bears the risk of the State's non-payment, regardless of cause, including but not limited to, the State's financial failure, bankruptcy, reorganization or other financial difficulty. In the event of the State's said non-payment, Vendor will be paid a pro rata share of the amount actually recovered from the State after deducting Knowledge Services' actual costs of recovery including attorneys' fees. No other fees, expenses, or benefits of any kind shall be paid by Knowledge Services or made available to Vendor unless expressly authorized and agreed to by Knowledge Services.
g. Knowledge Services may alter its rate, fee or pricing schedule upon notice to Vendor.
h. Vendor shall notify Knowledge Services of any payment discrepancies promptly upon receipt of its payment from Knowledge Services. It is Vendor's sole responsibility to enter pre-approved shift, bill rate differential, expense and/or sales tax information, if applicable, in the VMS prior to invoicing. Knowledge Services is not responsible for errors or omissions made by Vendor and will not retroactively modify time entries or invoices to correct Vendor errors or omissions.
i. Knowledge Services, at the direction of the State, reserves the right to deduct from amounts, which are or shall become due and payable to Vendor under this or any contract between Vendor and the State, any amounts, which are or shall become due and payable to the State by Vendor.
j. Knowledge Services, at the direction of the State, reserves the right to deduct from amounts, which are or shall become due and payable to Knowledge Services or the State by Vendor.
k. All rates and fees are quoted in US dollars, and all payments shall be made in US dollars. Knowledge Services reserves the right to modify its accounting policies from time to time.

4. **Intellectual Property.** All documents, records, programs, data, film, tape, articles, memoranda, and other materials not developed or licensed by Vendor prior to execution of this Agreement, but specifically developed under this Agreement shall be considered "work for hire," and Vendor transfers any ownership claim to Knowledge Services, who shall transfer any ownership claim to the State, whereby all such materials will be the property of the State. Use of these materials, other than related to Agreement performance by Vendor, without the prior written consent of Knowledge Services and the State, is prohibited. During the performance of this Agreement, Vendor shall be responsible for any loss of or damage to these materials developed for or supplied by the State and used to develop or assist in the services provided while the materials are in the possession of Vendor. Any loss or damage thereto shall be restored at Vendor's expense. Vendor shall provide Knowledge Services with full, immediate, and unrestricted access to the work product during the term of this Agreement, and Knowledge Services will in turn provide such full, immediate and unrestricted access to the work product to the State. All subcontractor agreements shall include this requirement.

5. **Space, Facilities and Equipment.**
   a. The State will provide (for the business purposes only): a laptop, internet access, workspace and copy facilities to Resources. Telephone is 'Bring Your Own Device' with the expectation that all Resources will have a smart phone for communication. Knowledge Services and the State will work with Vendor in the event a Resource has an ergonomic request and can be reasonably accommodated.
   b. With State authorization, Resource personnel may work offsite. If offsite work is authorized, the State and Knowledge Services/Vendor shall jointly agree on device usage.

6. **Vendor Role and Responsibilities.**
   a. Vendor shall be responsible for all employment-related issues, including but not limited to, Resource pay, benefits, PTO, statutory taxes and costs, discipline, performance, employee relations, and termination.
   b. Knowledge Services will track and report on Resource and Vendor performance to the State.

c. Vendor shall use E-Verify to determine Resource's eligibility to work in the United States.
d. Vendor will provide employment status (W2 or 1099), or eligibility to work under work H1-B, L1, L9 visa or other visa categories.
e. Upon request, Knowledge Services will complete visa letters as reasonably requested and provided by Vendor for the visa process. The State will not provide end-client visa letters, or any other documentation requested as part of the visa process, to Vendor or Resource.
f. Vendor shall comply with all statutes, laws, regulations, codes, orders, policies, rules and regulations of federal, state or municipal authorities applicable to the furnishing of Services as set forth in this Agreement. Vendor shall comply with all State and Knowledge Services policies and procedures provided to Vendor.
g. Contracted sub-vendor personnel shall not use their access to State staff for marketing purposes or to promote their company.

7. **Subcontractors.** Vendor may not enter into any subcontract for the work to be performed under this Agreement without the express written consent of Knowledge Services. This provision shall not apply to contracts of employment between Vendor and its employees. No more than one sub-vendor layer is permitted, unless otherwise approved by Knowledge Services in writing. Any sub-vendor must be approved on a requisition basis by Knowledge Services prior to submittal of a candidate. If the use of sub-vendors is approved by Knowledge Services, Vendor must provide to Knowledge Services, if requested, documentation of the actual pay rate to Resource(s) and sub-vendor in question. Knowledge Services reserves the right to bring subcontracted Resources directly into the MSP program, and convert its Resources to an alternate Program Vendor.

   Vendor is solely responsible for the performance of work under this Agreement. The approval of Knowledge Services for Vendor to subcontract for work under this Agreement shall not relieve Vendor in any way of its responsibility for performance of the work.

   If Knowledge Services does permit Vendor to subcontract services, all Subcontractors shall be bound by the terms and conditions set forth in this Agreement. Vendor shall remain responsible to Knowledge Services and the State for the performance of any sub-vendor. Vendor shall give Knowledge Services immediate notice in writing of any legal action or suit filed, and prompt notice of any claim made against Vendor by any Subcontractor, which may result in litigation related in any way to this Agreement, or which may affect the performance of duties under this Agreement. Vendor shall indemnify and hold harmless Knowledge Services and the State from and against any such claim, loss, damage, or liability as set forth in Section 20, the State Held Harmless.

8. **Resource Employment Status Validation Form**. Vendor shall complete the, "Knowledge Services MSP Resource Employment Status Validation Form," located on the State of Maine MSP Program Portal, for each Resource that is selected to work on behalf of the State prior to the start of Resource's assignment. Vendor shall upload this form into the system as specified by Knowledge Services prior to the start of Resource's assignment.

9. **Information Safeguard, Security, Background Checks, Debarment and Subcontractors.**
   a. Vendor, and all subcontractors, shall comply with information security requirements presented in Exhibit D – Debarment, Performance and Non-Collusion Form, Exhibit F IRS Safeguard Contract Language – Technology Services, and Exhibit G – State of Maine Vendor Confidentiality & Non-Disclosure Agreement. These contract terms shall be included in all subcontractor agreements.
   b. If Knowledge Services or the State advises Vendor that an IT Resource provided through this Agreement will have access to Federal Tax Information, Vendor may not enter into any subcontract or payroll agreement for the work to be performed by the IT Resource under this agreement without the express written consent of the State which will include the appropriate 45-day notification to the IRS. The 45-day notification process will be coordinated and executed by the State of Maine, Maine Revenue Services. This provision shall not apply to contracts of employment between Vendor and its employees. This provision shall not apply to engagements for IT Resources not handling Federal Tax Information.
   c. Vendor agrees to conduct or to have conducted a background check of any Resource placed on assignment at a State Agency, or State facility ("Facility"), prior to the start of Resource's assignment.

d. Vendor shall maintain records and files of information safeguard, security and background checks and make them available for state inspection as requested by the State.
e. Background checks shall be completed for verification of, but not limited to:
    1. Social security trace – verification of social security number;
    2. Federal Criminal history check; including all State and Counties of Residence for the past 7 years;
    3. E-Verify employment eligibility verification;
    4. Federal Exclusion and Debarment Screening (FACIS). Vendor shall confirm that Resources are not excluded from participation in any federal health care program (such as Medicare or any state Medicaid program) or debarred or otherwise prohibited from participating in federal procurement and non-procurement programs by checking the Department of Health and Human Services' Office of the Inspector General's List of Excluded Individuals/Entities (http://exclusions.oig.hhs.gov/search.html) and the General Service Administration's list of debarred Contractors (http://epls.arnet.gov). Screening of FACIS is valid for six (6) months prior to initial hire date. Vendor shall administer an updated FACIS check when temporary personnel have been assigned to Client for a period of twelve (12) months or more;
    5. Sex Offender Registry check for all states of residency in the past seven (7) years; and
    6. A Maine Revenue Services tax liability check, if applicable, will be initiated by the State, subject to Maine Revenue Services' policies regarding such checks, for all Resources on assignment at Maine Revenue Services, and/or for Resources on assignment at other State Agencies, if so directed by the applicable Agency.
f. If the State notifies Knowledge Services and Vendor that Vendor personnel will have access to protected health information, Vendor personnel must execute a Business Associate Agreement (Exhibit E) with the Department of Health and Human Services.
g. Resources may also be required to provide additional, relevant pre-assignment documents, at the request of a State Agency.
h. In the event an Agency requires fingerprinting, such fingerprint check requirements shall supersede the background check requirements (a) and (b) stated above.
i. Knowledge Services requires Vendor to use a background check company specified by Knowledge Services.
j. Reasons for determining that a Resource did not satisfactorily pass the background check include, but are not limited to, the below guidelines. Any exceptions to the below guidelines must be approved by Knowledge Services and the State.
        i. Candidates convicted of criminal felonies or misdemeanors involving dishonesty or a breach of trust, including burglary, larceny, embezzlement, counterfeiting, forgery, theft or robbery, shall be excluded from consideration.
        ii. Candidates convicted of criminal felonies or misdemeanors involving violent acts such as murder, assault, rape and battery shall be excluded from consideration.
k. Costs associated with background or fingerprint checks shall be the sole responsibility of the applicable Vendor. Background and fingerprint check results shall be effective for a period of thirty (30) days prior to Resource's assignment start date. In the case of a "break in service" from the State, a new background check must be completed. A background check is effective for a period of six (6) months, unless otherwise specified for assignments at a State hospital.
l. A background or fingerprint check may be required to be run each year for Resources on assignment, as measured from Resource's assignment start date, and as directed by the applicable Agency. In the event the Resource begins work for a new Agency or Facility during such time, a separate fingerprint check will be required. Additionally, assignments located at a State hospital, school or correctional facility may require a TB shot to be updated annually. In the event, this is not performed by the applicable Facility, Vendor will be responsible for such test.
m. In extremely rare instances, under only the approval of the State, it may be allowed for a Resource to begin an engagement contingent upon a passed background check. If the Resource does not pass the background check, the Resource will immediately be terminated. Vendor will not be compensated for hours worked by the Resource failing the background check, and no invoice will be submitted to the State for hours worked by the Resource failing the background check.

10. **Subletting, Assignment or Transfer.** Vendor shall not sublet, sell, transfer, assign, or otherwise dispose of this Agreement, or any portion thereof, or of its right, title, or interest therein, without the written approval of Knowledge Services. Such approval shall not in any case relieve Vendor of its responsibility for performance of work under this Agreement.

11. **Independent Capacity:** In the performance of this Agreement, Vendor shall act in the capacity of an independent contractor and not as an employee or agent of the State or Knowledge Services.

12. **Employment and Personnel.** Vendor shall not engage any person in the employ of any the State or Agency in a position that would constitute a violation of 5 MRSA § 18 or 17 MRSA § 3104. Vendor shall not engage on a full-time, part-time, or any other basis, during the period of this Agreement, any personnel who are, or have been, at any time during the period of this Agreement, in the employ of any the State or Agency, except regularly retired employees, without the written consent of the State Purchases Review Committee. Further, Vendor shall not engage on this project on a full-time, part-time, or any other basis, during the period of this Agreement, any retired employee of the State, who has not been retired for at least one year, without the written consent of the State Purchases Review Committee. Vendor shall cause the foregoing provisions to be inserted in any subcontract for any work covered by this Agreement, so that such provisions shall be binding upon each subcontractor, provided that the foregoing provisions shall not apply to contracts or subcontracts for standard commercial supplies or raw materials.

13. **State Employees Not to Benefit.** No individual employed by the State at the time this Agreement is executed, or any time thereafter, shall be admitted to any share or part of this Agreement, or to any benefit that might arise there from, directly or indirectly, that would constitute a violation of 5 MRSA § 18 or 17 MRSA § 3104. No other individual employed by the State at the time this Agreement is executed, or any time thereafter, shall be admitted to any share or part of this Agreement, or to any benefit that might arise there from, directly or indirectly, due to his employment by, or financial interest in, Vendor, or any affiliate of Vendor, without the written consent of the State Purchases Review Committee. Vendor shall cause the foregoing provisions to be inserted in any subcontract for any work covered by this Agreement so that such provisions shall be binding upon each Subcontractor, provided that the foregoing provisions shall not apply to contracts or subcontracts for standard commercial supplies or raw materials.

14. **Accounting, Records and Audit.**
    a. Vendor shall maintain all books, documents, payrolls, papers, accounting records, and other evidence pertaining to this Agreement, including interim reports and working papers, and make such materials available at its offices at all reasonable times during the period of this Agreement, and for a period of five (5) years following termination or expiration of the Agreement. If any litigation, claim or audit is started before the expiration of the 5-year period, the records must be retained until all litigation, claims or audit findings involving the agreement have been resolved.
    b. Unless Knowledge Services or the State specifies in writing a shorter period of time, Vendor agrees to preserve and make available all documents and records pertaining to this Agreement for a period of five (5) years from the date of termination of this Agreement.
    c. Records involving matters in litigation shall be kept for one year following the termination of litigation, including all appeals.

15. **Access to Public Records.** As a condition of accepting a contract for services under this section, a contractor must agree to treat all records, other than proprietary information, relating to personal services work performed under the contract as public records under the freedom of access laws to the same extent as if the work were performed directly by the department or agency. For the purposes of this subsection, "proprietary information" means information that is a trade secret or commercial or financial information, the disclosure of which would impair the competitive position of the contractor and would make available information not otherwise publicly available. Information relating to wages and benefits of the employees performing the personal services work under the contract and information concerning employee and contract oversight and accountability procedures and systems are not proprietary information. Vendor shall maintain all books, documents, payrolls, papers,

accounting records and other evidence pertaining to this Agreement and make such materials available at its offices at all reasonable times during the period of this Agreement and for such subsequent period as specified under Maine Uniform Accounting and Auditing Practices for Community Agencies (MAAP) rules. Vendor shall allow inspection of pertinent documents by the State or any authorized representative of the State of Maine or Federal Government, and shall furnish copies thereof, if requested. This subsection applies to contracts, contract extensions and contract amendments executed on or after October 1, 2009.

16. **Termination.** The performance of work under this Agreement may be terminated by Knowledge Services in whole or in part, whenever, for any reason Knowledge Services or the State shall determine that such termination is in the best interests of Knowledge Services or the State. Any such termination shall be effected by the delivery to Vendor of a Notice of Termination specifying the extent to which the performance of work under this Agreement is terminated, and the date on which such termination becomes effective.

    Upon receipt of the Notice of Termination, Vendor shall:
    a. Stop work under this Agreement on the date and to the extent specified in the Notice of Termination;
    b. Take such action as may be necessary, or as Knowledge Services or the State may direct, for the protection and preservation of the property, information, and data related to this Agreement, which is in the possession of Vendor, and in which Knowledge Services or the State has, or may acquire, an interest;
    c. Terminate all orders to the extent that they relate to the performance of the work terminated by the Notice of Termination;
    d. Assign to the State in the manner, and to the extent directed by Knowledge Services, all of the rights, titles, and interests of Vendor under the orders so terminated, in which case the State shall have the right, at its discretion, to settle or pay any or all claims arising out of the termination of such orders;
        1. With the approval of Knowledge Services and the State, settle all outstanding liabilities and claims, arising out of such termination of orders, the cost of which would be reimbursable in whole or in part, in accordance with the provisions of this Agreement;
        2. Transfer title to Knowledge Services, who shall transfer to the State (to the extent that title has not already been transferred) and deliver in the manner, at the times, and to the extent directed by the State, equipment and products purchased pursuant to this Agreement, and all files, source code, data manuals, or other documentation, in any form, that relate to all the work completed, or in progress, prior to the Notice of Termination;
        3. Complete the performance of such part of the work as shall not have been terminated by the Notice of Termination; and
        4. Proceed immediately with the performance of the preceding obligations, notwithstanding any delay in determining or adjusting the amount of any compensation under this section.

    Notwithstanding the above, nothing herein shall limit the right of Knowledge Services or the State to pursue any other legal remedies against Vendor.

17. **Governmental Regulations.** Vendor shall comply with all applicable governmental ordinances, laws, and regulations.

18. **Governing Law.** This Agreement shall be governed by, interpreted, and enforced in accordance with the laws, statutes, and regulations of the State of Maine, without regard to conflicts of law provisions. The provisions of the United Nations Convention on Contracts for the International Sale of Goods and of the Uniform Computer Information Transactions Act shall not apply to this Agreement. Any legal proceeding against Knowledge Services or the State regarding this Agreement shall be brought in the State of Maine in a court of competent jurisdiction.

19. **State Held Harmless.** Vendor shall indemnify and hold harmless Knowledge Services and the State and its officers, agents, and employees from and against any and all claims, liabilities, and costs, including reasonable attorney fees, for any or all injuries to persons or property or claims for money damages, including claims for violation of intellectual property rights, arising from the negligent acts or omissions of Vendor, its employees or

agents, officers or Subcontractors in the performance of work under this Agreement; provided, however, Vendor shall not be liable for claims arising out of the negligent acts or omissions of Knowledge Services or the State, or for actions taken in reasonable reliance on written instructions of Knowledge Services or the State.

20. **Limitation of Liability.** Vendor's liability for damages sustained by the State or Knowledge Services as the result of Vendor's default or acts or omissions in the performance of work under this Agreement, whether such damages arise out of breach, negligence, misrepresentation, or otherwise, shall be no greater than:
    a. Damages for violation or infringement of any copyright or trademark;
    b. Damages for bodily injury (including death) to persons, and damages for physical injury to tangible personal property or real property; and
    c. The amount of any other actual direct damages up to the greater of $500,000 or three times the value of the Product or Service that is the subject of the claim, up to a maximum of $25,000,000. For example, if the Product or Service that is the subject of the claim was valued at $15,000,000, then Vendor would be liable for no more than $25,000,000. For purposes of this subsection, the term "Product" would typically include the following, but not be limited to, Materials, Source Code, Machine Code, and Licenses.

    Notwithstanding the above, neither party shall be liable for any indirect or consequential damages.

21. **Notice of Claims.** Vendor shall give Knowledge Services immediate notice in writing of any legal action or suit filed related in any way to this Agreement, or which may affect the performance of duties under this Agreement, and prompt notice of any claim made against Vendor by any Subcontractor, which may result in litigation related in any way to this Agreement, or which may affect the performance of duties under this Agreement.

.

22. **Insurance Requirements.** Vendor shall procure and maintain, for the duration of the Agreement, insurance against claims for injuries to persons, or damages to property, which may arise from, or in connection with, the fulfillment of this Agreement by Vendor, its agents, representatives, employees, or Subcontractors.
    a. **Minimum Coverage**
        1. Commercial general liability (including products, completed operations, and broad-form contractual): $1,000,000 per occurrence;
        2. Workers' Compensation and employer's liability: as required by law;
        3. Professional liability: $1,000,000; and
        4. Property (including contents coverage for all records maintained pursuant to this Agreement): $1,000,000 per occurrence.
    b. **Other Provisions.** Unless explicitly waived by Knowledge Services, the insurance policies should contain, or be endorsed to contain, the following provisions:
        1. Vendor's insurance coverage shall be the primary insurance. Any insurance or self- insurance maintained by the State for its officers, agents, and employees shall be in excess of Vendor's insurance and shall not contribute to it.
        2. Vendor's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.
        3. Vendor shall furnish Knowledge Services with certificates of insurance and with those endorsements, if any, effecting coverage required by these Insurance Requirements. The certificates and endorsements for each insurance policy are to be signed by a person authorized by the insurer to bind coverage on its behalf. All certificates and endorsements are to be received and approved by Knowledge Services before this Agreement commences. Knowledge Services reserves the right to require complete, certified copies of all required insurance policies at any time.
        4. If allowable by policy, all policies should contain a revised cancellation clause allowing thirty (30) days' notice to Knowledge Services in the event of cancellation for any reason including nonpayment.

23. **Non-Appropriation.** Notwithstanding any other provision of this Agreement, if the State does not receive sufficient funds to pay for the work to be performed under this Agreement, if funds are de-appropriated, or if the State does not receive legal authority to expend funds from the Maine the State Legislature or Maine courts,

then the State is not obligated to make payment to Knowledge Services, and thereby Vendor, under this Agreement.

24. **Severability.** The invalidity or unenforceability of any particular provision, or part thereof, of this Agreement shall not affect the remainder of said provision, or any other provisions, and this Agreement shall be construed in all respects as if such invalid or unenforceable provision or part thereof had been omitted.

25. **Force Majeure.** Either party may be excused from the performance of an obligation under this Agreement in the event that performance of that obligation by a party is prevented by an act of God, act of war, riot, fire, explosion, flood, or other catastrophe, sabotage, severe shortage of fuel, power or raw materials, change in law, court order, national defense requirement, strike or labor dispute, provided that any such event, and the delay caused thereby, is beyond the control of, and could not reasonably be avoided by that party. Upon the occurrence of an event of force majeure, the time period for performance of the obligation excused under this section shall be extended by the period of the excused delay, together with a reasonable period, to reinstate compliance with the terms of this Agreement.

26. **Set-Off Rights.** The State shall have all of its common law, equitable, and statutory rights of set-off. These rights shall include, but not be limited to, the State's option to withhold for the purposes of set-off any monies ultimately due to Vendor under this Agreement, up to any amounts due and owing to the State with regard to this Agreement, any other Agreement with any the State department or agency, including any Agreement for a term commencing prior to the term of this Agreement, plus any amounts due and owing to the State for any other reason including, without limitation, tax delinquencies, fee delinquencies, or monetary penalties relative thereto. The State shall exercise its set-off rights in accordance with normal the State practices including, in cases of set-off pursuant to an audit, the finalization of such audit by the State agency, its representatives, or the State Controller, and Knowledge Services shall provide notification to Vendor of such.

27. **Advertising and Publications.** Vendor shall not publish any statement, news release, or advertisement pertaining to this Agreement without the prior written approval of the Knowledge Services. Should this Agreement be funded, in whole or in part, by Federal funds, then in compliance with the Steven's Amendment, it will be clearly stated when issuing the Statements, press releases, requests for proposals, bid solicitations, and other documents: (1) the percentage of the total cost that was financed with Federal moneys; and (2) the dollar amount of Federal funds.

28. **Conflict of Interest.** Vendor certifies that it presently has no interest and shall not acquire any interest which would conflict in any manner or degree with the performance of its services hereunder. Vendor further certifies that in the performance of this Agreement, no person having any such known interests shall be employed.

29. **State Property.** Vendor shall be responsible for the proper custody and care of any State or the State owned property furnished for Vendor's use in connection with the performance of this Agreement, and Vendor will reimburse the State for its loss or damage, normal wear and tear excepted.

30. **Patent, Copyright and Other Intellectual Property Rights**
    a. Vendor certifies that all services, equipment, software, supplies, and any other products provided under this Agreement do not, and will not, infringe upon or violate any patent, copyright, trade secret, or any other proprietary right of any third party. In the event of any claim by a third party against Knowledge Services or the State, Knowledge Services shall promptly notify Vendor and Vendor, at its expense, shall defend, indemnify, and hold harmless Knowledge Services and/or the State against any loss, cost, expense, or liability arising out of such claim, including reasonable attorney fees.
    b. Vendor may not publish or copyright any data without the prior approval of the State. The State and the Federal Government, if applicable, shall have the right to publish, duplicate, use, and disclose all such data in any manner, and for any purpose whatsoever, and may authorize others to do so.

31. **State IT Policies.** All IT products and services delivered as part of this Agreement must conform to the State IT Policies, Standards, and Procedures (Maine.Gov/oit/oitpolicies) effective at the time this Agreement is executed.

32. **Confidentiality.**
    a. All materials and information given to Vendor by the State, or acquired by Vendor on behalf of the State, whether in verbal, written, electronic, or any other format, shall be regarded as confidential information.
    b. In conformance with applicable Federal and the State statutes, regulations, and ethical standards, Vendor and the State shall take all necessary steps to protect confidential information regarding all persons served by the State, including the proper care, custody, use, and preservation of records, papers, files, communications, and any such items that may reveal confidential information about persons served by the State, or whose information is utilized in order to accomplish the purposes of this Agreement.
    c. In the event of a breach of this confidentiality provision, Vendor shall notify the Agreement Administrator immediately.
    d. Vendor shall comply with the Maine Public Law, Title 10, Chapter 210-B (Notice of Risk to Personal Data Act).

33. **Miscellaneous.**
    a. All Exhibits referred to in this Agreement are attached hereto and made a part hereof for all purposes.
    b. This Agreement may not be assigned by either party without the other party's prior written consent; provided, however, that either party may assign this Agreement, with notice, consent and approval of the other party, or delegate the performance of all or part of its obligations and duties hereunder, to an Affiliate (provided the party guaranty the Affiliate's performance). As used herein, "Affiliate" of a party shall mean any corporation or other business entity controlled by, controlling or under common control with, such entity.
    c. Each provision of this Agreement shall be considered severable and if, for any reason, any provision hereof is determined to be invalid and contrary to, or in conflict with, any existing or future law or regulation by any court or agency having valid jurisdiction, such provision shall be given the maximum permissible effect, and such invalidity or illegality shall not impair the operation or affect the remaining provisions of this Agreement; and the latter shall continue to be given full force and effect and bind the parties hereto and such invalid provisions shall be deemed not to be a part of this Agreement.
    d. This Agreement constitutes the complete understanding of the parties regarding the Services. No amendment, modification or waiver of any provision of this Agreement shall be valid unless in writing and signed by both parties. Any failure or delay by either party in exercising any right or remedy shall not be deemed a waiver of any further, prior, or future right or remedy hereunder.
    e. This Agreement may be signed in two counterparts, each of which shall be deemed to be an original, but all of which together shall form a single agreement.

IN WITNESS WHEREOF, the parties hereto have caused their duly authorized officer to execute this Agreement as of the date first written above.

GuideSoft, Inc. dba Knowledge Services

By: _____ By:_____

Name: _____ Name: _____

Title: _____ Title: _____

Exhibit A
Program Rates and Fees

1. **Hourly Rates by Position.** Current maximum or not-to-exceed bill rates by position will be posted at https://www.maine.gov/dafs/bbm/procurementservices/reports/statewide-contracts/information-technology-managed-staffing-program.

2. **Rate Differentials.**
   a. Overtime shall generally be billed at a "straight-time rate," and overtime rate differentials will only be billed if so communicated by Knowledge Services. Overtime is defined as work performed in excess of 40 hours per week, or as otherwise defined by applicable law, and only for the positions specified under this Agreement, or specified in the job posting or requisition released by Knowledge Services. The overtime rate differential, if any, will be communicated to Vendor in the job posting or requisition released by Knowledge Services.
   b. There shall not be any other pay or shift premium rates, including but not limited to holiday or weekend time, unless specified in the job posting or requisition released by Knowledge Services.

3. **Resource Conversion.** If the State determines that it would be in the State's best interest to hire a Resource of Vendor after a period of nine hundred and sixty (960) hours, Knowledge Services will require that Vendor will release the selected Resource from any non-competition agreements that may be in effect. This release will be at no cost to the State or Vendor or Resource.

   If the State determines that it would be in the State's best interest to hire a resource of Vendor prior to completion of a period of nine hundred and sixty (960) hours, the State will notify Knowledge Services, who in turn will notify the Vendor, of the State's intent to hire the Resource. Knowledge Services will require that Vendor release the selected Resource from any non-competition agreements that may be in effect, and will negotiate a conversion fee with Vendor, which shall not exceed the maximum rates detailed below:

Hours Worked	0-160 hours	>160-320 hours	>320-480 hours	>480-640 hours	>640-800 hours	>800-960 hours	>960 hours
Maximum/not to exceed conversion fee	20% of first year annual salary*	15% of first year annual salary*	12.5% of first year annual salary*	10% of first year annual salary*	7.5% of first year annual salary*	5% of first year annual salary*	0% of first year annual salary*

The first year annual salary will be the annual salary that would be paid to Resource by the State during the first year of service, exclusive of any benefits or fees paid to the Resource.

Exhibit B

Posting and Response Processes

I. Vendor Participation in the Program.

a) Incumbent Workers. The hours worked by Resources who were assigned to the State prior to the Contract Effective Date (each, an "Incumbent Worker"), if any, on the assignments they were given prior to the Contract Effective Date (the "Incumbent Assignments") shall be billed at the rate communicated to Vendor by Knowledge Services and as entered into the VMS, as of the Contract Effective Date. Notwithstanding the foregoing, Knowledge Services shall have no liability to Vendor for, and Vendor hereby agrees to defend, indemnify and hold harmless Knowledge Services from, any liability of any kind arising out of or related to (1) any services or invoices of the Vendor provided to the State prior to the Contract Effective Date, if any, or (2) the exceptions regarding the Incumbent Workers expressly stated herein, if any, to Vendor's obligations.

II. Postings.

a) Submission to Vendor. Knowledge Services will receive Postings from the State and may, at Knowledge Services' discretion, forward such Postings to Vendor.

b) Content.

i. Generally. Postings may set forth (i) the name or position of the State personnel placing the Posting with Knowledge Services, (the "Hiring Manager") requesting a Resource, (ii) the applicable the State personnel who must approve the timecard of each Resource if different than the Hiring Manager (the "Time Approver"), (iii) if necessary, any other the State personnel responsible for the State's oversight of the Resource, (iv) project description, (v) start date under such Posting (the "Posting Start Date"); and (vi) Skill Set of the Resource requested

ii. Posting - Specific. Postings shall also set forth any job-specific information, including, by way of example, (i) any applicable Pay-Rate limitation, (ii) anticipated duration of project, (iii) anticipated project completion date, (iv) travel requirements, if any, (v) the State cost elements or units to which time and expenses should be charged, (vi) assignments for charging of time and expenses, and (vii) the assigned the State business unit at the assigned Facility where the Resource filing the Posting will report for the applicable assignment.

c) Posting Communication Procedure. Knowledge Services shall deliver Postings to Vendor via its VMS. Vendor shall, at its own cost, obtain and maintain necessary equipment and personnel to receive process and respond to Postings submitted through the communication procedure used by Knowledge Services as amended from time to time.

III. Resources.

a) Pre-Start Duties. For each Resource selected, prior to the applicable Posting Start Date, Vendor shall:

i. deliver to Knowledge Services any information about such Resource (including resume or background information), which Knowledge Services reasonably requested in the applicable Posting;

ii. obtain and provide to Knowledge Services completed pre-start documentation for such Resource, as set forth in the Agreement;

iii. perform the screening, background checking and drug testing procedures set forth in the Agreement; and

iv. prepare for onboarding of such selected Resource as set forth in the Agreement.

b) Former Employees. Vendor shall indicate, or require each applicable Resource candidate to indicate, in response to a Posting whether a Resource candidate is a former employee of the State. Vendor acknowledges and agrees that former employees of the State may only perform services for the State as a Resource with the prior approval of the State.

Exhibit C

Vendor Service Level Agreements

The Vendor Service Level Agreement (SLA) shall govern this Agreement for Services. The goals, descriptions, calculations, and target shall be strictly adhered to, and any penalties defined below shall be enforced in this agreement. Additional SLAs may be added in the sole discretion of Knowledge Services, and shall be communicated to Vendor in writing.

Service Level Agreement (SLA)	Vendor Goal	Frequency	Description	Calculation	Target
Normal Resume Submittal Response Time	4 business days	Quarterly	Measures average response time from release of requirement to Vendor to Knowledge Services' receipt of first round of screened candidate resumes	Number of NE requisitions which received first round of resumes for review within 4 business days/ total number of NE requisitions.	90.0% or higher
Normal Round 1 Fill Rate	N/A	Quarterly	Measures Vendor's ability to satisfactorily fulfill requisitions within first round of resumes submitted to Knowledge Services (normal requisitions).	Total number of NE engagements resulting from the first round of resumes / total number of NE engagements.	80.0% or higher
Urgent Resume Submittal Response Time	2 business days	Quarterly	Measures average response time from release of requirement to Vendor to Knowledge Services' receipt of first round of screened candidate resumes – (*an urgent requirement is needed in less than 10 business days*)	Number of NE URGENT requisitions that received first batch of resumes for review within 2 business days / total number of NE URGENT requisitions.	92.0% or higher
Urgent Round 1 Fill Rate	N/A	Quarterly	Measures Vendor's ability to fulfill requisitions within first round of resumes submitted to Knowledge Services (URGENT requisitions).	Total number of NE URGENT filled positions resulting from the first round of resumes / total number of NE requisitions filled.	90.0% or higher
Normal On-Boarding Response Time	2 Business Days	Quarterly	Measures Vendor's ability to satisfactorily schedule the resources to be on-boarded after selection is made.	Candidate start date notification to Knowledge Services within 2 days of candidate selection / total number of candidates started	90% or higher
Attrition Rate	N/A	Annual	Measures Resource turnover due to unplanned situations that are not caused by the State, not including inadequate performance, death, and serious illness of the resource. Applicable situations include Resource leaving for another position.	Number of unplanned turnovers from NE Resources in period reviewed / total number of NE Resources in the period reviewed. (Resources that are entering time in the period reviewed).	7.0% or lower
Performance Removal	N/A	Semi-annual (6-months)	Measures Resource turnover due to inadequate resource performance.	Number of turnovers from NE Resources in the period reviewed /	5.0% or lower

Service Level Agreement (SLA)	Vendor Goal	Frequency	Description	Calculation	Target
				total number of NE Resources in the period reviewed. (Resources that are entering time in the period reviewed).	

All SLAs will be reviewed quarterly unless any single SLA fails the target, whereupon monthly review will be implemented. A discussion will take place between Knowledge Services and Vendor, Vendor will be given a warning, and a plan will be developed to improve on the deficient SLA(s) and to reach the minimum achievement target by the next quarter. If the next quarterly review of the deficient SLA shows no improvement, Vendor will be placed on probation and will be given 3 months after the date of the quarterly review to show improvement in the SLA that failed. If the SLA is not met after the next quarterly review, Knowledge Services will assess Vendor to determine, at its sole discretion, whether this Agreement should be terminated. ***Notwithstanding the foregoing, Knowledge Services reserves the right to terminate this Agreement at any time in its sole discretion.***

Exhibit D
Debarment Form

[Page intentionally left blank]

DEBARMENT, PERFORMANCE, and NON-COLLUSION CERTIFICATION

Vendor Name: _____ Date: _____

Certification Regarding
Debarment, Suspension and Other Responsibility Matters
Primary covered Transactions

This Certification is required by the Regulations implementing Executive Order 12549, Debarment and Suspension, 29 CFR Part 98, Section 98.510, Participants' Responsibilities. The Regulations were published as Part VII of the May 26, 1998 Federal Register (pages 19160-19211).

(BEFORE SIGNING THIS CERTIFICATION, PLEASE READ THE ATTACHED INSTRUCTIONS WHICH ARE AN INTEGRAL PART OF THE CERTIFICATION)

1. The prospective primary participant certifies to the best of its knowledge and belief that it and its principles:

    a. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;
    b. Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction, violation of Federal or State anti-trust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
    c. Are not presently indicted for or otherwise criminally or civilly charged by a government entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph 1.b of this Certification; and
    d. Have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State or local) terminated for cause or default.

2. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

_____

Name and Title, Authorized Representative

_____

Signature

Instructions for Certification

1. By signing and submitting this proposal, the prospective primary participant is providing the Certification set out below.

2. The inability of a person to provide the Certification required below will not necessarily result in denial of participation in this covered transaction. The prospective participant shall submit an explanation of why it cannot provide the Certification set out below. The Certification or explanation will be considered in connection with the Office of Information Technology (OIT) determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a Certification or an explanation shall disqualify such person from participation in this transaction.

3. The Certification in this clause is material representation of fact upon which reliance was placed when the Office of Information Technology (OIT) determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous Certification, in addition to other remedies available to the Federal Government, the Office of Information Technology (OIT) may terminate this transaction for cause of default.

4. The prospective primary participant shall provide immediate written notice to the Office of Information Technology (OIT) if at any time the prospective primary participant learns its Certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

5. The terms “covered transaction”, “debarred”, “suspended”, “ineligible”, “lower tier covered transaction”, “participant”, “person”, “primary covered transaction”, “principal”, “proposal”, and “voluntarily excluded”, as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549. You may contact the Office of Information Technology (OIT) for assistance in obtaining a copy of these regulations.

6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the Office of Information Technology (OIT).

7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled “Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transactions” provided by the Office of Information Technology (OIT), without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Lists of Parties Excluded from Procurement or Nonprocurement Programs.

9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the Office of Information Technology (OIT) may terminate this transaction for cause or default.

Exhibit E
Business Associate Agreement

[Page intentionally left blank]

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made this ___ day of _____, 20xx (the "Effective Date") by and between the State of Maine, Department of Health and Human Services (the Covered Entity, hereinafter, the "Department") and _____("Business Associate"), together (the "Parties"); and

WHEREAS, Business Associate may use, disclose, create, receive, maintain or transmit protected health information in a variety of form or formats, including verbal, paper and electronic (together, "PHI") on behalf of the Department in connection with Business Associate's performance of its obligations under the following agreement between the parties: _____ dated _____, 20xx (the "Underlying Agreement"); and

WHEREAS, the Parties intend to ensure the confidentiality, privacy and security of Department's PHI as required by law, including the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191 (HIPAA), and its implementing regulations at 45 CFR Parts 160 and 164 (the Privacy, Security, Breach Notification and Enforcement Rules or "HIPAA Rules") as updated by the Health Information Technology for Economic and Clinical Care Act (HITECH) enacted under Title XII of the American Recovery and Reinvestment Act of 2009, and its implementing Regulations (together, the "HIPAA and HITECH Rules"); and

WHEREAS, the Parties agree that certain federal and state laws, rules, regulations and accreditation standards also impose confidentiality restrictions that apply to this business relationship, and may include, but are not limited to: 42 CFR 2 *et. seq;,* 5 M.R.S.A. §19203-D; 22 M.R.S.A. §§42, 261, 815, 824, 833, 1494, 1596, 1711-C, 1828, 3173, 3292, 4008, 5328, 7250, 7703, 8754; 10 M.R.S.A 1346 *et. seq*; 34-B M.R.S.A. §1207; 14-193 C.M.R, Ch. 1, Part A, § IX; and applicable accreditation standards of The Joint Commission or other appropriate accreditation body regarding confidentiality.

NOW THEREFORE, the parties agree as follows:

Specific Definitions for the Purpose of this Agreement:

Breach means the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such PHI. A security or privacy incident that involves PHI is presumed to be a breach requiring notification unless the Department proves, through specific risk analysis steps, that there is a low probability that the PHI was compromised or a) the incident does not involved unsecured PHI, or b) the incident falls into another exception or safe harbor as set forth in the HIPAA and HITECH Rules.

Business Associate is a person or entity that creates, receives, maintains or transmits PHI on behalf of, or provides services to, a covered entity, as set forth in the HIPAA Rules and other than in the capacity of a workforce member.

Covered Entity is a 1) health plan, (2) health care clearinghouse, or 3) health care provider who electronically transmits any health information in connection with transactions for which HHS has adopted standards. Generally, these electronic transactions concern billing and payment for services or insurance coverage.

Designated Record Set means the billing and medical records about individuals maintained by or for a covered provider: the enrollment, claims adjudication, payment, case or medical management record systems maintained by or for a health plan; or that are used in whole, or in part, by the covered entity to make decisions about individuals.

Individual means the person who is the subject of the PHI.

Protected Health Information means information that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and is transmitted or maintained in electronic or any other form or medium.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information [or PHI] or interference with system operation in an information system.

Subcontractor means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private, to whom a business associate has delegated a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services ("HHS") in its guidance.

General Definitions. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA and HITECH Rules: Data Aggregation, Disclosure, Health Care Operations, Minimum Necessary, Notice of Privacy Practices, Required by Law, and Use.

1. Permitted Uses and Disclosures

a. Business Associate agrees to use or disclose the PHI authorized by this Agreement only to perform the services of the Underlying Agreement between the Parties, or as required by law.

b. Business Associate may use or disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, only where a) the use or disclosure does not violate any law governing the protection of the PHI, including, but not limited to, prohibitions under 42 CFR Part 2 (Part 2 Regulations), and b) the disclosures are required by law or c) Business Associate agrees only to disclose the minimum necessary PHI to accomplish the intended purpose and i) obtains reasonable assurances from the person or entity to whom the information is disclosed that the PHI will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity, and ii) the person or entity agree to immediately notify Business Associate of any instances of which it is aware that the confidentiality, privacy or security of the information has been actually or potentially breached.

c. Business Associate may provide data aggregation services relating to the health care operations of the Department, or de-identify the Department's PHI, only when such specific services are permissible under the Underlying Agreement or as otherwise preapproved in writing by the Department.

2. Obligations and Activities of the Business Associate

a. *Compliance.* Business Associate agrees to comply with the HIPAA and HITECH Rules, and other applicable state or federal law, to ensure the protection of the Department's PHI, and only use and disclose PHI consistent with the Department's minimum necessary policy and the legal requirements of this Agreement. Business Associate may not use or disclose PHI in a manner that would violate the HIPAA or HITECH Rules or other state or federal law if performed by the Department.

b. *Safeguards*. In complying with the HIPAA and HITECH Rules, Business Associate agrees to use appropriate administrative, technical and physical safeguards, and comply with any required security or privacy obligations, to protect the confidentiality, integrity and availability of the Department's PHI.

c. *Reporting.* Business Associate agrees to report to the Department any inappropriate use or disclosure of the Department's PHI of which it becomes aware, i.e. any use or disclosure not permitted in this Agreement or in violation of any legal requirement, including actual and suspected breaches of unsecured PHI, and any actual or potential security incident of which it becomes aware. Such report will be made to the Department's Director of Healthcare Privacy or her designee within twenty-four (24) hours of when the Business Associate becomes aware of an actual or suspected incident or breach. In the event that a breach is determined to have occurred under the authority of the Business Associate, Business Associate will cooperate promptly with the Department to provide all specific information required by the Department for mandatory notification purposes.

d. *Subcontractors and Agents.* In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associate shall ensure that any third parties, agents or subcontractors (together, "Subcontractors") that use, disclose, create, acquire, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI. Business Associate shall obtain and maintain a written agreement with each Subcontractor that has or will have access, through Business Associate, to the Department's PHI, ensuring that the Subcontractor agrees to be bound to the same restrictions, terms and conductions that apply to Business Associate under this Agreement.

e. *Mitigation.* The Business Associate shall exhaust, at its sole expense, all reasonable efforts to mitigate any harmful effect known to the Business Associate arising from the use or disclosure of PHI by Business Associate in violation of the terms of this Agreement.

f. *Accounting of Disclosures*. To the extent required by the terms of this Agreement, Business Associate will maintain and make available the information and/or documentation required to provide an accounting of disclosures as necessary to satisfy the Department's obligations under 45 CFR 164.528.

g. *Access.* In the event that Business Associate creates or maintains PHI in a designated record set, Business Associate will use commercially reasonable efforts to make PHI available in the format requested, and as necessary to satisfy the Department's obligation under 45 C.F.R. 164.524, within 30 days from the time of request. Business Associate will inform the Department of the individual's request within 5 (five) business days of the request.

h. *Amendment*. In the event that Business Associate creates or maintains PHI in a designated record set, Business Associate agrees to make any amendment(s) to the PHI as directed or agreed to by the Department, or take other measures as necessary to satisfy the Department's obligations under 45 CFR 164.526, in such time period and in such manner as the Department may direct.

i. *Restrictions*. Upon notification from the Department, Business Associate shall adhere to any restrictions on the use or disclosure of PHI agreed to by or required of the Department pursuant to 45 CFR 164.522.

j. *Audit by the Department or the HHS Secretary*. The Business Associate will make its internal practices, books and records relating to the use or disclosure of PHI received from the Department or used, acquired, maintained, created or received by the Business Associate on behalf of the Department, available to either the Department or the HHS Secretary for the purposes of determining the compliance of either the Department or the Business Associate with the Medicaid Act, and the HIPAA and HITECH Rules, or any other federal, state or accreditation requirement. 45 C.F.R. 164.504.

k. *Other Obligations*: To the extent that Business Associate is to carry out one or more of the Department's obligations under the HIPAA and HITECH Rules or other federal or state law, Business Associate agrees to comply with the legal requirements that apply to the Department in performing that obligation;

3. Obligations of the Department

a. The Department shall notify Business Associate of a) any limitation in any applicable Notice of Privacy Practices that would affect the use or disclosure of PHI by the Business Associate and b) any changes, revocations, restrictions or permissions by an individual to the use and disclosure of his/her PHI to which the Department has agreed, to the extent such restrictions or limitations may affect the performance of Business Associate's services on behalf of the Department.

b. The Department shall not request that Business Associate use or disclose PHI in any format, and in any manner, that would be prohibited if performed by the Department.

4. Hold Harmless

Business Associate agrees to indemnify and hold harmless the Department, its directors, officers, agents, shareholders, and employees against any and all claims, demands, expenses, liabilities or causes of action that arise from any use or disclosure of PHI not specifically permitted by this Agreement, applicable state or federal laws, licensing, accreditation or other requirements.

5. Term of Agreement

a. *Term*. This Agreement shall be effective as of the Effective Date and shall terminate at the end of the term of the Underlying Agreement. To the extent that the Underlying Agreement automatically renews, this Agreement shall also automatically renew itself for the same renewal period unless the Department terminates this Agreement for cause as set forth in Section 5(c). Either party may terminate the Agreement consistent with the written notice provision regarding termination in the Underlying Agreement.

b. *Auto-renewal.* In the event that this Agreement is automatically renewed, the Business Associate agrees to be bound by the terms of this Agreement and laws referenced in this Agreement that are current and in effect at the time of renewal.

c. *Termination for Cause*. Notwithstanding the foregoing, Business Associate authorizes termination of this Agreement by the Department if the Department determines that Business Associate has violated a material term of the Agreement. The Department shall either, at its sole discretion:

i. Provide the Business Associate an opportunity to cure or end the violation within a time frame and upon such conditions as established by the Department; and

ii. Immediately terminate this Agreement in the event the Business Associate has either failed to cure in the time frame provided by the Department or if cure is not possible.

d. *Obligations of the Business Associate upon Termination*. Upon termination of this Agreement for any reason, Business Associate, shall

i. Return or destroy all PHI used, created, accessed, acquired, maintained, or received by the Business Associate on behalf of the Department, and retain no copies in any format. Business Associate shall ensure that its Subcontractors do the same.

ii. If the Department agrees that Business Associate may destroy all PHI in its possession, Business Associate shall certify such destruction to the Department.

iii. If returning or destroying PHI is not feasible, Business Associate agrees to protect the confidentiality of the PHI and retain only that PHI which is necessary for the Business Associate to continue its proper management and administration, or to carry out its legal responsibilities. Business Associate shall not use or disclose the PHI for other than the purpose for which it was retained, and return to the Department, or destroy if approved by the Department, such PHI when no longer required. Furthermore, Business Associate shall continue to use appropriate safeguards and comply with the HIPAA and HITECH Rules, other applicable state and federal law, with respect to PHI in any format for as long as Business Associate retains the PHI.

iv. Upon appropriate direction from the Department, Business Associate shall transmit the PHI to another business associate of the Department consistent with all legal and regulatory safeguards delineated in this Agreement.

6. Qualified Service Organization Agreement

To the extent that in performing its services for or on behalf of the Department, Business Associate uses, discloses, maintains or transmits PHI that is protected by the Part 2 Regulations, Business Associate acknowledges that it is a Qualified Service Organization for the purpose of such federal law; acknowledges that in receiving, storing, processing or otherwise dealing with any such patient records, it is fully bound by the Part 2 Regulations; and, if necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Part 2 Regulations.

7. Survival of Business Associate Obligations

The obligations of the Business Associate under this Agreement shall survive the termination of this Agreement indefinitely.

8. Miscellaneous

a. *Amendment*. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Department to comply with the requirements of the HIPAA and HITECH Rules, and/or other applicable laws or requirements. This Agreement may only be amended in writing, signed by authorized representatives of the Parties.

b. *Injunction.* The Department and Business Associate agree that any violation of the provisions of this Addendum may cause irreparable harm to the Department. Accordingly, in addition to any other remedies available to the Department, Department shall be entitled to seek an injunction or other decree of specific performance with respect to any violation of this Agreement or explicit threat thereof, without bond or other security being required and without the necessity of demonstrating actual damages.

c. *Interpretation*. Any ambiguity in this Agreement shall be resolved to ensure that the Department is in compliance with the HIPAA and HITECH Rules, or other applicable laws or privacy or security requirements.

d. *Legal References.* A reference in this Agreement to a section in the HIPAA or HITECH Rules or to other federal or state law, means the section as in effect or as amended.

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the Effective Date.

	Department		Business Associate
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____

Exhibit F

IRS SAFEGUARD CONTRACT LANGUAGE
CONTRACT LANGUAGE FOR GENERAL SERVICES

[Page intentionally left blank]

IRS SAFEGUARD CONTRACT LANGUAGE
CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.

(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material 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 by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(8) (Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material 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 by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to 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/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 $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 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 information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Exhibit G

State of Maine
Department of Administrative and Financial Services
Office of Information Technology (OIT)
Vendor Confidentiality & Non-Disclosure Agreement (Form A)

[Page intentionally left blank]

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES
OFFICE OF INFORMATION TECHNOLOGY (OIT)
VENDOR CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT (FORM A)

THIS CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT ("Agreement"), is between the Maine State Office of Information Technology ("OIT"), having a principal place of business at 51 Commerce Drive, Augusta, Maine 04330, and _____ ("Vendor") with its principal place of business at _____ as of _____, 20 (the Effective Date).

WHEREAS, the State of Maine has engaged the Vendor to provide services in connection with the operation or management of certain State of Maine programs or services pursuant to MA 18P 2020 ("Contract"); and

WHEREAS, in connection with the performance of the Contract, Vendor has access to confidential information (as defined below); and

WHEREAS, OIT wishes to ensure the protection of Confidential Information and restrict the Vendor's use of Confidential Information to purposes directly connected and necessary for the performance of the Contract; and

WHEREAS, the Vendor recognizes the need to restrict disclosure and use of Confidential Information.

NOW THEREFORE, in consideration of the above premises and for other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the Parties agree as follows:

1.Definitions. For the purposes of this Agreement, the following terms shall be defined as follows:

A. Authorized Person

"Authorized Person" is defined as a person authorized by OIT as having a need to receive, possess, store, access, view and/or use Confidential Information for an Authorized Use.

B. Authorized Use

"Authorized Use" is defined as the use of Confidential Information by the Vendor or Authorized Persons, solely for the purpose of performing the Contract.

C. Confidential Information

Information that belongs to OIT or resides on the State of Maine information technology infrastructure, includes highly sensitive and confidential data. In many instances, improper release or use of this information by an OIT or other state employee or third-party provider is a crime. "Confidential Information" includes any and all information disclosed to, or otherwise acquired or observed by, the Vendor, including their respective employees, agents and subcontractors (all of the foregoing collectively referred to as "Representatives"), from or through OIT or any agency, instrumentality or political subdivision of the State of Maine Government, including but not limited to:

1) Any information that describes the State of Maine architecture, design, access authentication, encryption or security of information technology infrastructure, systems and software (1 MRSA§400 et seq.);
2) Tax information protected by 36 M.R.S.A §191 and the Internal Revenue Code, 26 U.S.C.§§6103, 7213, 7213A, 7413 regarding unauthorized disclosure or inspection of tax information.State and federal statutes may impose substantial civil and criminal penalties for

unauthorized access or disclosure and carry monetary penalties of varying amounts, and/or imprisonment for up to 5 years, together with the costs of prosecution;
3) Protected health information and personally identifiable information received by the State from the Centers for Medicare and Medicaid Services and the Social Security Administration, and any other sources, that is protected under state and federal healthcare and privacy laws(including but not limited to the following: 22 MRSA §1711-C; the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 104th Congress; the federal Privacy Act of 1974, 5 U.S.C. § 552a, as amended; section 1106 of the Social Security Act, as amended; the Patient Protection and Affordable Care Act of 2010 (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152); the E-Government Act of 2002, as amended; related Centers for Medicare & Medicaid Services and Social Security Administration regulations and policies, as well as other relevant privacy federal statutes, rules, regulations and guidance;
4) Criminal Justice Information records maintained by the Federal Bureau of Investigation Criminal Justice Information Services Division, as well as any other state and federal criminal records information protected by various state and federal statutes. Violations may subject the disclosing party to civil penalties imposed by federal Privacy Act of 1974, 5 U.S.C. § 552a, as amended, for unauthorized disclosure or inspection of criminal record information;
5) Any sensitive information that may be protected pursuant to any other federal or state statutory or regulatory scheme intention to protect information, or by order, resolution or determination of a court or administrative board or other administrative body;
6) Any information that has been designated as confidential and not subject to disclosure pursuant to the Maine Freedom of Access Act (1 MRSA § 400 et seq.); and
7) Any information that OIT or the State, regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., OIT, other state agencies, state employees, electronic systems, or third party contractors) provides to Vendor, or which Vendor obtains, discovers, derives or otherwise becomes aware of as a result of the Agreement other than:

a) information that is previously rightfully known to Vendor on a non-confidential basis without restriction on disclosure;
b) information that is or becomes, from no act or failure to act on the part of the Vendor, generally known in the relevant industry or in the public domain from a source other than the Vendor, OIT or any agency, instrumentality or political subdivision of the State of Maine Government, provided that such source is not bound by a confidentiality agreement or is not otherwise prohibited from transferring the information to the Vendor by a contractual, legal or fiduciary duty; or
c) information that is independently developed by the Vendor without the use of or benefit from Confidential Information and such independent development can be documented by the Vendor.

D. Electronic Information

“Electronic Information” is defined as information or data produced or stored by electronic, digital, or similar means.

E. Services

“Services” is defined as the services to be performed by the Vendor in connection with the operation or management of the Contract.

F. Vendor

"Vendor" is defined to include the Vendor and the Vendor's respective employees, agents and subcontractors assigned by Vendor to perform obligations under the Contract (all of the foregoing collectively referred to as "Representatives").

2. Duty to Protect Confidential Information.

In consideration for the ability to perform the Services, the Vendor shall hold all Confidential Information in confidence and protect that Confidential Information with the same standard of care required to keep its own similar information confidential, and must abide by all commercially reasonable administrative, physical, and technical standards for maintaining this information confidential (e.g., standards established by the National Institute of Standards and Technology). In addition, the Vendor must safeguard all Confidential Information from unauthorized access, loss, theft, destruction, and the like. The Vendor may not, without prior consent from OIT, disclose any Confidential Information to any person for any reason at any time; provided, however it is understood that the Vendor may disclose Confidential Information to its Representatives and its business, financial and legal advisors who require the Confidential Information for the purpose of evaluating or performing the Services on the condition that, prior to such disclosure, the Representatives and advisers have been advised of the confidential and non-public nature of the Confidential Information and are subject to a written confidentiality agreement that contains restrictions and safeguards at least as restrictive as those contained in this Agreement. The Vendor shall be responsible for any breach of this Agreement by any of the Vendor's Representatives or advisors.

The Vendor shall promptly report any activities by any individual or entity that the Vendor suspects may compromise the availability, integrity, security or privacy of any Confidential Information. The Vendor shall notify OIT immediately upon becoming aware that Confidential Information is in the possession of or has been disclosed to an unauthorized person or entity.

3. Discovery and Notification of Breach of Confidential Information

In the event of a breach of security or suspected security incident, intrusion, unauthorized use or disclosure involving Confidential Information, the Vendor shall notify OIT by telephone call (207-624-7700) and email to the OIT information security team (Security.Infrastructure@maine.gov) within the following timeframes:

A. Upon the discovery of a breach of security or suspected security incident involving Confidential Information in electronic, or any other medium if the information was, or is reasonably believed to have been, acquired by an unauthorized person; or

B. Within twenty-four (24) hours of the discovery of any suspected security incident, intrusion, unauthorized use or disclosure of Confidential Information in violation of this Agreement, or potential loss of Confidential Information affecting this Agreement.

Notification shall also be provided to the OIT Contract Manager and the OIT Information Security Officer. The Vendor shall provide a written report of all information known at the time. The Vendor shall take:

A. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

B. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

4.Written Report

In addition to the report required above, the Vendor shall provide a written report of the investigation to the OIT Chief Information Security Officer within ten (10) working days of the discovery of the breach of security or suspected security incident, or unauthorized use or disclosure involving Confidential Information. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

5. Notification to individuals.

The Vendor shall notify individuals of the breach or unauthorized use or disclosure of Confidential Information when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. Any notification provided must first be approved by the OIT Chief Information Security Officer, who shall approve the time, manner and content of any such notifications prior to their release.

6. Press Releases.

The Vendor shall not issue any press releases, give or make any presentations, or give to any print, electronic or other news media information regarding his/her Contract or engagement under this Agreement- nor shall Vendor authorize or permit any other person or entity to do so - without the prior express written permission of OIT. Vendor shall immediately refer any media requests or other requests for information to the Director of Communications, Department of Administrative and Financial Services (207) 624-7800.

7. Use Restriction.

Vendor shall not receive, possess, store, access, view and/or use Confidential Information for any reason or purpose other than as strictly necessary in regard to the performance of the Services. Vendor shall not permit unauthorized persons or entities to gain access to Confidential Information and shall not divulge methods of accessing Confidential Information to unauthorized persons.

8. Security Obligations Regarding Confidential Information.

The Vendor agrees to comply with the following security obligations as well as any other such obligations specified in the contract or conveyed to him/her during the course of the Agreement. The Vendor agrees to:

A. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any Confidential Information that is created, received, maintained, used, possessed, stored, accessed, viewed and/or transmitted on behalf of OIT or through OIT or any agency, instrumentality or political subdivision of the State of Maine Government;
B. Continually monitor its operations and take any action necessary to assure that Confidential Information is safeguarded in accordance with OIT policies and standards and all applicable federal and state laws and regulations;
C. Unless otherwise authorized by OIT, not to store Confidential Information on personal (i.e., non-OIT / non-Vendor) computing or other electronic or mobile storage devices or taken or removed in any form from OIT;
D. Comply with all applicable federal and State laws and regulations;
E. Comply with all OIT policies and procedures including but not limited to those that provide for accessing, protecting and preserving State assets;
F. Hold all Confidential Information in the strictest confidence;

G. Obtain fingerprint-based criminal history record checks for all Vendor's employees, agents and subcontractors when requested by OIT pursuant to federal and state statutory and regulatory directives, at the expense of the vendor;
H. Make reasonable efforts to comply with any request by OIT to conduct an audit, including a request to audit the Vendor's third-party or contractor work;
I. Not to intrude upon, disrupt or deny services to OIT; and
J. Use only those access rights granted by OIT.

9. Certification by Vendor of Return of Confidential Information, Electronic Information and Tangible Property.

Promptly following the written request of OIT, and immediately upon termination of the Services, the Vendor shall return all Confidential Information stored on any format to OIT or destroy any Confidential Information that Vendor possesses in a format that cannot be returned. Further, vendor agrees to submit to OIT on Vendor's letterhead a "CERTIFICATION OF RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION, ELECTRONIC INFORMATION, AND TANGIBLE PROPERTY" certifying that all copies of Confidential Information, electronic property and tangible property belonging to the State of Maine or OIT have been returned, or if necessary destroyed, using the form provided in Appendix A.

10. Termination.

Vendor's Authorized Use of Confidential Information shall terminate automatically upon: (a) breach of this Agreement as determined solely by OIT, (b) completion or termination of Vendor's services, or, (c) termination of the Vendor's Contract, whichever occurs first.

11. Remedies.

In the event of any breach or threatened breach of this Agreement, the State of Maine shall have all equitable and legal rights (including the right to obtain injunctive relief and specific performance) to seek redress for such breach, prevent further breaches and to be fully compensated (including litigation costs and reasonable attorney's fees) for losses or damages resulting from such breach. The Vendor acknowledges that compensation for damages may not be sufficient and that injunctive relief to prevent or limit any breach of confidentiality is a remedy available to the State of Maine.

12. Governing Law.

This Agreement shall be governed by and construed in accordance with the laws of the State of Maine. The place of this Agreement, its situs and forum, shall be Kennebec County, Maine, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of Maine and stipulates that the State Courts in Kennebec County shall be the proper venue for all matters. If any provision of the Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the other provisions shall remain in full force and effect.

13. Entire Agreement.

This Agreement constitutes the entire agreement with respect to the Confidential Information disclosed hereunder and supersedes all prior or contemporaneous oral or written agreements concerning such Confidential Information. This Agreement is intended to be read in harmony with any other confidentiality and non-disclosure provisions contained within the Contract.

IN WITNESS WHEREOF, the Parties have executed this Agreement through their duly authorized representatives effective as of the Effective Date set forth above.

:

By: _____

Printed:_____

Title: _____

Date: _____

Address:_____

_____

State of Maine Office of Information Technology:

By: _____

Printed:_____

Title: _____

Date: _____

Address:_____

_____

APPENDIX A

CERTIFICATION OF RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION, ELECTRONIC INFORMATION, AND TANGIBLE PROPERTY BY VENDOR PURSUANT TO VENDOR CONFIDENTIALITY & NONDISCLOSURE AGREEMENT

DATED _____

Pursuant to the Vendor Confidentiality and Non-Disclosure Agreement between the State of Maine, acting by and through the Office of Information Technology ("OIT") and _____ ("Vendor") dated _____, Vendor acknowledges his/her responsibility to return or destroy all Confidential Information upon termination of the Vendor's services to OIT. This document certifies that all copies of Confidential Information, electronic property and tangible property belonging to the State of Maine or OIT have been returned, or if necessary destroyed, as described below: _____

Description of returned Confidential Information, electronic information or tangible property:

_____

_____

_____

Description of destroyed Confidential Information, electronic information or tangible property:

_____

_____

_____

_____

Vendor Signature

_____

Vendor Name

_____

Date

_____

.