Alternate Contract Source (ACS)
No. 43230000-NASPO-16-ACS
For
Cloud Solutions

This Alternate Contract Source No. 43230000-NASPO-16-ACS for Cloud Solutions (Contract), is between the Department of Management Services (Department), an agency of the State of Florida (State), located at 4050 Esplanade Way, Tallahassee, FL 32399 and Visionary Integration Professionals, LLC (Contractor), located at 80 Iron Point Circle, Suite 100, Folsom, CA 95630, collectively referred to herein as the "Parties."

WHEREAS, the Department is authorized by section 287.042(16), Florida Statutes:

To evaluate contracts let by the Federal Government, another state, or a political subdivision for the provision of commodities and contract services, and, if it is determined by the Secretary of the Department of Management Services in writing to be cost-effective and the best value to the state, to enter into a written agreement authorizing an agency to make purchases under such contract;

WHEREAS, the State of Utah, acting by and through the National Association of State Procurement Officials (NASPO) ValuePoint, competitively procured Cloud Solutions and executed Contract No. AR3116, Cloud Solutions (Master Contract), with the Contractor;

WHEREAS, the Secretary evaluated the Master Contract and determined that use of the Master Contract is cost-effective and the best value to the state.

NOW THEREFORE, in consideration of the mutual promises contained herein, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. **Term and Effective Date.**

The Master Contract became effective on March 11, 2019, and its term currently ends on September 15, 2026. The Master Contract has no renewals available. The Contract will become effective on the date signed by all Parties. The Contract will expire on September 15, 2026, unless terminated earlier or renewed in accordance with Exhibit B, Special Contract Conditions.

2. **Order of Precedence.**

This Contract document and the attached exhibits constitute the Contract and the entire understanding of the Parties. Exhibits A, B, C, D, and this Contract document constitute the Participating Addendum to the Master Contract and modify or supplement the terms

and conditions of the Master Contract. All exhibits listed below are incorporated by reference into, and form part of, this Contract. In the event of a conflict, the following order of precedence shall apply:

a) This Contract document
b) Exhibit A, Additional Special Contract Conditions
c) Exhibit B, Special Contract Conditions
d) Exhibit C, Master Contract (including any amendments made prior to the effective date of this Contract and any subsequent amendments added to this Contract in accordance with the Modifications Section listed below)
e) Exhibit D, Contractor Selection Justification Form

Where the laws and regulations of a state other than the State of Florida are cited or referenced in the Master Contract, such citation or reference shall be replaced by the comparable Florida law or regulation.

3. Purchases off this Contract.

Upon execution of this Contract, agencies, as defined in section 287.012, Florida Statutes, may purchase products and services under this Contract. Any entity making a purchase off of this Contract acknowledges and agrees to be bound by the terms and conditions of this Contract. The Contractor shall adhere to the terms included in any contract or purchase orders issued pursuant to this Contract.

4. Primary Contacts.

Department's Contract Manager:
John (Jake) Goodrich
Division of State Purchasing
Florida Department of Management Services
4050 Esplanade Way, Suite 360
Tallahassee, Florida 32399-0950
Telephone: (850) 487-9847
Email: john.goodrich@dms.fl.gov

Contractor's Contract Manager:
Visionary Integration Professionals, LLC
Jennifer Salazar, Director of Contracts
80 Iron Point Circle, Suite 100
Folsom, CA 95630
916-985-9625
legal@trustvip.com

5. Cloud Computing Requirements

Contractor agrees to cooperate with the Department and Customers and perform all actions necessary to assist with all tasks in furtherance of the Department's and/or Customer's efforts to comply with the obligations under Rule Titles 60FF and 60GG, Florida Administrative Code (F.A.C.), as applicable. This includes, but is not limited to, adherence to the cloud computing requirements set forth in Rule Chapter 60GG-4, F.A.C.

6. Authorization

Approval of this Participating Addendum by the State Chief Procurement Official and State Chief Information Officer is an authorization for participation in the NASPO cooperative contract process; it is not intended as an approval of any specific purchase or solution. It is the responsibility of the Customer to validate all terms and conditions and to ensure compliance with all applicable statutes and rules.

7. Request for Quotes

Customers purchasing Cloud Solutions from this Participating Addendum shall create a Request for Quote (RFQ), each time they desire to purchase Cloud Solutions. The Customer shall issue a detailed RFQ to the ACS Contractor(s) who offer(s) the applicable cloud solution(s). The specific format of the RFQ is left to the discretion of the Customer, but must contain the following:

a) Applicable service and deployment model(s);
b) Data security classification;
c) Service level agreement requirements; and
d) Exit strategy considerations.

8. Contractor Selection Justification Form.

Customers purchasing Cloud Solutions from this Participating Addendum shall attach to the purchase order a completed Contractor Selection Justification Form (Exhibit D) of this Participating Addendum, incorporated herein by reference and accessible at: https://www.dms.myflorida.com/business_operations/state_purchasing/state_contracts_and_agreements/alternate_contract_source/cloud_solutions/forms.

9. Modifications.

Any amendments to this Contract must be in writing and signed by the Parties. If amendments are made to the Master Contract after the effective date of this Contract, the Contractor shall: 1) notify the Department of such amendments; and 2) provided the Department is amenable to incorporating the amendments into this Contract, enter into a written amendment with the Department reflecting the addition of such amendments to this Contract.

Alternate Contract Source (ACS)
No. 43230000-NASPO-16-ACS
For
Cloud Solutions

IN WITNESS THEREOF, the Parties hereto have caused this Contract to be executed by their duly authorized undersigned officials.

CONTRACTOR
Visionary Integration Professionals, LLC

DocuSigned by:
Jennifer Salazar
CA553197AB0346E...

Name: Jennifer Salazar

Title: Director of Contracts

10/28/2022 | 6:25 PM EDT
Date:

DEPARTMENT OF MANAGEMENT SERVICES

DocuSigned by:
Pedro Allende
5E91A9D369EB47C...

Pedro Allende

Secretary

11/1/2022 | 11:06 AM EDT
Date:

Department of MANAGEMENT SERVICES
We serve those who serve Florida

EXHIBIT A

ADDITIONAL SPECIAL CONTRACT CONDITIONS

The Contractor and agencies, as defined in section 287.012, Florida Statutes acknowledge and agree to be bound by the terms and conditions of the Master Contract except as otherwise specified in the Contract, which includes the Special Contract Conditions and these Additional Special Contract Conditions.

A. Orders: Contractor must be able to accept the MyFloridaMarketPlace (MFMP) purchase orders.

B. Contractor and Subcontractors, Affiliates, Partners, Resellers, Distributors, and Dealers: By execution of a Contract, the Contractor acknowledges that it will not be released of its contractual obligations to the Department or state agencies because of any failure of an affiliate, partner, subcontractor, reseller, distributor, or dealer. The Contractor is responsible for ensuring that its affiliates, partners, subcontractors, resellers, distributors, and dealers providing commodities and performing services in furtherance of the Contract do so in compliance with the terms and conditions of the Contract. The Contractor is fully responsible for satisfactory completion of all work performed under the Contract.

C. Purchases Prerequisites: Contractor must ensure that entities receiving payment directly from Customers under this Contract must have met the following requirements:
   - Have an active registration with the Florida Department of State, Division of Corporations (www.sunbiz.org), or, if exempt from the registration requirements, provide the Department with the basis for such exemption.
   - Be registered in the MFMP Vendor Information Portal (https://vendor.myfloridamarketplace.com).
   - Have a current W-9 filed with the Florida Department of Financial Services (https://flvendor.myfloridacfo.com)

D. MFMP Electronic Invoicing: The Contractor may supply electronic invoices in lieu of paper-based invoices for those transactions processed through MFMP. Electronic invoices may be submitted to the agency through one of the mechanisms as listed below:

   1) EDI (Electronic Data Interchange)
   This standard establishes the data contents of the Invoice Transaction Set (810) for use within the context of an Electronic Data Interchange (EDI) environment. This transaction set can be used for invoicing via the Ariba Network (AN) for catalog and non-catalog goods and services.

   2) PO Flip via AN
   This online process allows Contractors to submit invoices via the AN for catalog and

non-catalog goods and services. Contractors have the ability to create an invoice directly from their inbox in their AN account by simply "flipping" the PO into an invoice. This option does not require any special software or technical capabilities.

The Contractor grants the State and the third-party provider of MFMP, a State contractor, the right and license to use, reproduce, transmit, distribute, and publicly display Contractor's information within MFMP. In addition, the Contractor grants the State and the third-party provider the right and license to reproduce and display within MFMP the Contractor's trademarks, system marks, logos, trade dress, or other branding designation that identifies the products made available by the Contractor under the Contract.

The Contractor will work with the MFMP management team to obtain specific requirements for the electronic invoicing if needed.

E. Contract Reporting: The Contractor shall provide the Department the following accurate and complete reports associated with this Contract.

1) Contract Quarterly Sales Reports. The Contractor shall submit complete Quarterly Sales Reports to the Department's Contract Manager within 30 calendar days after the close of each State fiscal quarter (the State's fiscal quarters close on September 30, December 31, March 31, and June 30).

   Reports must be submitted in MS Excel using the DMS Quarterly Sales Report Format, which can be accessed at https://www.dms.myflorida.com/business_operations/state_purchasing/vendor_resources/quarterly_sales_report_format. Initiation and submission of the most recent version of the Quarterly Sales Report posted on the DMS website is the responsibility of the Contractor without prompting or notification from the Department's Contract Manager. If no orders are received during the quarter, the Contractor must email the DMS Contract Manager confirming there was no activity.

2) Certified and Minority Business Enterprises Reports. Upon Customer request, the Contractor shall report to each Customer spend with certified and other minority business enterprises in the provision of commodities or services related to the Customer orders. These reports shall include the period covered; the name, minority code, and Federal Employer Identification Number of each minority business enterprise utilized during the period; commodities and services provided by the minority business enterprise; and the amount paid to each minority business enterprise on behalf of the Customer.

3) Ad Hoc Sales Reports. The Department may require additional Contract sales information such as copies of purchase orders or ad hoc sales reports. The Contractor shall submit these documents and reports in the format acceptable to the Department and within the timeframe specified by the Department.

4) MFMP Transaction Fee Reports. The Contractor shall submit complete monthly MFMP Transaction Fee Reports to the Department. Reports are due 15 calendar days after the end of each month. Information on how to submit MFMP Transaction Fee Reports online can be located at https://www.dms.myflorida.com/business_operations/state_purchasing/myfloridamarketplace/mfmp_vendors/transaction_fee_and_reporting. Assistance with transaction fee reporting is also available by email at feeprocessing@myfloridamarketplace.com or telephone at 866-FLA-EPRO (866-352-

3776) from 8:00 a.m. to 6:00 p.m. Eastern Time.

F. Financial Consequences: The Department reserves the right to impose financial consequences when the Contractor fails to comply with the requirements of the Contract. The following financial consequences will apply for the Contractor's non-performance under the Contract. The Customer and the Contractor may agree to add additional Financial Consequences on an as-needed basis beyond those stated herein to apply to that Customer's resultant contract or purchase order. The State of Florida reserves the right to withhold payment or implement other appropriate remedies, such as Contract termination or nonrenewal, when the Contractor has failed to comply with the provisions of the Contract. The Contractor and the Department agree that financial consequences for non-performance are an estimate of damages which are difficult to ascertain and are not penalties.

The financial consequences below will be paid and received by the Department of Management Services within 30 calendar days from the due date specified by the Department. These financial consequences below are individually assessed for failures over each target period beginning with the first full month or quarter of the Contract performance and every month or quarter, respectively, thereafter.

Financial Consequences Chart

Deliverable	Performance Metric	Performance Due Date	Financial Consequence for Non-Performance (Per Calendar Day Late/Not Received by the Contract Manager)
Contractor will timely submit complete Quarterly Sales Reports	All Quarterly Sales Reports will be submitted timely with the required information	Completed reports are due on or before the 30th calendar day after the close of each State fiscal quarter	$250
Contractor will timely submit complete MFMP Transaction Fee Reports	All MFMP Transaction Fee Reports will be submitted timely with the required information	Completed reports are due on or before the 15th calendar day after the end of each month	$100

No favorable action will be considered when Contractor has outstanding Contract Quarterly Sales Reports, MFMP Transaction Fee Reports, or any other documentation owed to the Department or Customer, to include fees / monies, that is required under this Contract.

G. Business Review Meetings: Both the Department and Customer reserve the right to schedule business review meetings. The Department or Customer may specify the format

or agenda for the meeting. At a minimum, the Business Review Meeting may include the following topics:

a. Contract compliance
b. Contract savings (in dollar amount and cost avoidance)
c. Spend reports by Customer
d. Recommendations for improved compliance and performance

H. Special Contract Conditions revisions: the corresponding subsections of the Special Contract Conditions referenced below are replaced in their entirety with the following:

2.2 Renewal.
Upon written agreement, the Department and the Contractor may renew the Contract in whole or in part only as set forth in the Contract documents, and in accordance with section 287.057(14), F.S.

3.7 Transaction Fees.
The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(24), F.S. All payments issued by Customers to registered Vendors for purchases of commodities or contractual services will be assessed Transaction Fees as prescribed by rule 60A-1.031, F.A.C., or as may otherwise be established by law. Vendors must pay the Transaction Fees and agree to automatic deduction of the Transaction Fees when automatic deduction becomes available. Vendors will submit any monthly reports required pursuant to the rule. All such reports and payments will be subject to audit. Failure to comply with the payment of the Transaction Fees or reporting of transactions will constitute grounds for declaring the Vendor in default and subject the Vendor to exclusion from business with the State of Florida.

5.1 Conduct of Business.
The Contractor must comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor must comply with section 274A of the Immigration and Nationality Act, the Americans with Disabilities Act, Health Insurance Portability and Accountability Act, if applicable, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status. The provisions of subparagraphs 287.058(1)(a)-(c) and (g), F.S., are hereby incorporated by reference.

Nothing contained within this Contract shall be construed to prohibit the Contractor from disclosing information relevant to performance of the Contract or purchase order to members or staff of the Florida Senate or Florida House of Representatives.

Pursuant to section 287.057(26), F.S., the Contractor shall answer all questions of, and ensure a representative will be available to, a continuing oversight team.
The Contractor will comply with all applicable disclosure requirements set forth in section 286.101, F.S. In the event the Department of Financial Services issues the Contractor a final order determining a third or subsequent violation pursuant to section 286.101(7)(c), F.S., the Contractor shall immediately notify the Department and applicable Customers and shall be disqualified from Contract eligibility.

5.4 Convicted, Discriminatory, Antitrust Violator, and Suspended Vendor Lists.

In accordance with sections 287.133, 287.134, and 287.137, F.S., the Contractor is hereby informed of the provisions of sections 287.133(2)(a), 287.134(2)(a), and 287.137(2)(a), F.S. For purposes of this Contract, a person or affiliate who is on the Convicted Vendor List, the Discriminatory Vendor List, or the Antitrust Violator Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Contract. The Contractor must notify the Department if it or any of its suppliers, subcontractors, or consultants have been placed on the Convicted Vendor List, the Discriminatory Vendor List, or the Antitrust Violator Vendor List during the term of the Contract.

In accordance with section 287.1351, F.S., a vendor placed on the Suspended Vendor List may not enter into or renew a contract to provide any goods or services to an agency after its placement on the Suspended Vendor List.

A firm or individual placed on the Suspended Vendor List pursuant to section 287.1351, F.S., the Convicted Vendor List pursuant to section 287.133, F.S., the Antitrust Violator Vendor List pursuant to section 287.137, F.S., or the Discriminatory Vendor List pursuant to section 287.134, F.S., is immediately disqualified from Contract eligibility.

5.6 Cooperation with Inspector General and Records Retention.
Pursuant to section 20.055(5), F.S., the Contractor understands and will comply with its duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor must provide any information the Inspector General deems relevant. Such information may include, but will not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Contract. The Contractor will retain such records for the longer of five years after the expiration or termination of the Contract, or the period required by the General Records Schedules maintained by the Florida Department of State, at the Department of State's Records Management website. The Contractor agrees to reimburse the State of Florida for the reasonable costs of investigation incurred by the Inspector General or other authorized State of Florida official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State of Florida which results in the suspension or debarment of the Contractor. Such costs will include but will not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor agrees to impose the same obligations to cooperate with the Inspector General and retain records on any subcontractors used to provide goods or services under the Contract.

8.1.1 Termination of Contract.
The Department may terminate the Contract for refusal by the Contractor to comply with this section by not allowing access to all public records, as defined in Chapter 119, F.S., made or received by the Contractor in conjunction with the Contract unless the records are exempt from s. 24(a) of Art. I of the State Constitution and section 119.071(1), F.S.

8.1.2 Statutory Notice.
Pursuant to section 119.0701(2)(a), F.S., for contracts for services with a contractor acting on behalf of a public agency, as defined in section 119.011(2), F.S., the following applies:

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE

CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE DEPARTMENT'S CUSTODIAN OF PUBLIC RECORDS AT PUBLICRECORDS@DMS.FL.GOV, (850) 487-1082 OR 4050 ESPLANADE WAY, SUITE 160, TALLAHASSEE, FLORIDA 32399-0950.

Pursuant to section 119.0701(2)(b), F.S., for contracts for services with a contractor acting on behalf of a public agency as defined in section 119.011(2), F.S., the Contractor shall:

(a) Keep and maintain public records required by the public agency to perform the service.

(b) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.

(c) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the Contract term and following the completion of the Contract if the Contractor does not transfer the records to the public agency.

(d) Upon completion of the Contract, transfer, at no cost, to the public agency all public records in possession of the Contractor or keep and maintain public records required by the public agency to perform the service. If the Contractor transfers all public records to the public agency upon completion of the Contract, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the Contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the public agency, upon request from the public agency's custodian of public records, in a format that is compatible with the information technology systems of the public agency.

12.1 Performance or Compliance Audits.
The Department may conduct or have conducted performance and/or compliance audits of the Contractor and subcontractors as determined by the Department. The Department may conduct an audit and review all the Contractor's and subcontractors' data and records that directly relate to the Contract. To the extent necessary to verify the Contractor's fees and claims for payment under the Contract, the Contractor's agreements or contracts with subcontractors, partners, or agents of the Contractor, pertaining to the Contract, may be inspected by the Department upon fifteen (15) calendar days' notice, during normal working hours and in accordance with the Contractor's facility access procedures where facility access is required. Release statements from its subcontractors, partners, or agents are not required for the Department or its designee to conduct compliance and performance audits on any of the Contractor's contracts relating to this Contract. The Inspector General, in accordance with section 5.6, the State of Florida's Chief Financial Officer, and the Office of the Auditor General shall also have authority to perform audits and inspections.

13.2 E-Verify.
The Contractor and its subcontractors have an obligation to utilize the U.S. Department of Homeland Security's (DHS) E-Verify system for all newly hired employees in accordance with section 448.095, F.S. By executing this Contract, the Contractor certifies that it is registered with, and uses, the E-Verify system for all newly hired employees in accordance with section 448.095, F.S. The Contractor must obtain an affidavit from its subcontractors in accordance with paragraph (2)(b) of section 448.095, F.S., and maintain a copy of such affidavit for the duration of the Contract. The Contractor shall provide a copy of its DHS Memorandum of Understanding (MOU) to the Department's Contract Manager within five days of Contract execution.

This section serves as notice to the Contractor regarding the requirements of section 448.095, F.S., specifically sub-paragraph (2)(c)1, and the Department's obligation to terminate the Contract if it has a good faith belief that the Contractor has knowingly violated section 448.09(1), F.S. If terminated for such reason, the Contractor will not be eligible for award of a public contract for at least one year after the date of such termination. The Department will promptly notify the Contractor and order the immediate termination of the contract between the Contractor and a subcontractor performing work on its behalf for this Contract should the Department have a good faith belief that the subcontractor has knowingly violated section 448.09(1), F.S.

I. Special Contract Conditions additions: the following subsection is added to the Special Contract Conditions:

12.3 Document Inspection.
In accordance with section 216.1366, F.S., the Department or a state agency is authorized to inspect the: (a) financial records, papers, and documents of the Contractor that are directly related to the performance of the Contract or the expenditure of state funds; and (b) programmatic records, papers, and documents of the Contractor which the Department or state agency determines are necessary to monitor the performance of the Contract or to ensure that the terms of the Contract are being met. The Contractor shall provide such records, papers, and documents requested by the Department or a state agency within 10 Business Days after the request is made.

Exhibit B

SPECIAL CONTRACT CONDITIONS
JULY 1, 2019 VERSION

Table of Contents

In accordance with Rule 60A-1.002(7), F.A.C., Form PUR 1000 is included herein by reference but is superseded in its entirety by these Special Contract Conditions.

SECTION 1. DEFINITION.

The following definition applies in addition to the definitions in Chapter 287, Florida Statutes (F.S.), and Rule Chapter 60A-1, Florida Administrative Code (F.A.C.):

1.1 Customer.
The agency or eligible user that purchases commodities or contractual services pursuant to the Contract.

SECTION 2. CONTRACT TERM AND TERMINATION.

2.1 Initial Term.
The initial term will begin on the date set forth in the Contract documents or on the date the Contract is signed by all Parties, whichever is later.

2.2 Renewal.
Upon written agreement, the Department and the Contractor may renew the Contract in whole or in part only as set forth in the Contract documents, and in accordance with section 287.057(13), F.S.

2.3 Suspension of Work and Termination.

2.3.1 Suspension of Work.
The Department may, at its sole discretion, suspend any or all activities under the Contract, at any time, when it is in the best interest of the State of Florida to do so. The Customer may suspend a resulting contract or purchase order, at any time, when in the best interest of the Customer to do so. The Department or Customer will provide the Contractor written notice outlining the particulars of the suspension. After receiving a suspension notice, the Contractor must comply with the notice and will cease the performance of the Contract or purchase order. Suspension of work will not entitle the Contractor to any additional compensation. The Contractor will not resume performance of the Contract or purchase order until so authorized by the Department.

2.3.2 Termination for Convenience.
The Contract may be terminated by the Department in whole or in part at any time, in the best interest of the State of Florida. If the Contract is terminated before performance is completed, the Contractor will be paid only for that work satisfactorily performed for which costs can be substantiated. Such payment, however, may not exceed an amount which is the same percentage of the Contract price as the amount of work satisfactorily performed. All work in progress will become the property of the Customer and will be turned over promptly by the Contractor.

2.3.3 Termination for Cause.
If the performance of the Contractor is not in compliance with the Contract requirements or the Contractor has defaulted, the Department may:

(a) immediately terminate the Contract;
(b) notify the Contractor of the noncompliance or default, require correction, and specify the date by which the correction must be completed before the Contract is terminated; or
(c) take other action deemed appropriate by the Department.

SECTION 3. PAYMENT AND FEES.

3.1 Pricing.
The Contractor will not exceed the pricing set forth in the Contract documents.

3.2 Price Decreases.
The following price decrease terms will apply to the Contract:

3.2.1 Quantity Discounts. Contractor may offer additional discounts for one-time delivery of large single orders;

3.2.2 Preferred Pricing. The Contractor guarantees that the pricing indicated in this Contract is a maximum price. Additionally, Contractor's pricing will not exceed the pricing offered under comparable contracts. Comparable contracts are those that are similar in size, scope, and terms. In compliance with section 216.0113, F.S., Contractor must annually submit an affidavit from the Contractor's authorized representative attesting that the Contract complies with this clause.

3.2.3 Sales Promotions. In addition to decreasing prices for the balance of the Contract term due to a change in market conditions, the Contractor may conduct sales promotions involving price reductions for a specified lesser period. The Contractor must submit documentation identifying the proposed: (1) starting and ending dates of the promotion, (2) commodities or contractual services involved, and (3) promotional prices compared to then-authorized prices.

3.3 Payment Invoicing.
The Contractor will be paid upon submission of invoices to the Customer after delivery and acceptance of commodities or contractual services is confirmed by the Customer. Invoices must contain sufficient detail for an audit and contain the Contract Number and the Contractor's Federal Employer Identification Number.

3.4 Purchase Order.
A Customer may use purchase orders to buy commodities or contractual services pursuant to the Contract and, if applicable, the Contractor must provide commodities or contractual services pursuant to purchase orders. Purchase orders issued pursuant to the Contract must be received by the Contractor no later than the close of business on the last day of the Contract's term. The Contractor is required to accept timely purchase orders specifying delivery schedules that extend beyond the Contract term even when such extended delivery will occur after expiration of the Contract. Purchase orders shall be valid through their specified term and performance by the Contractor, and all terms and conditions of the Contract shall survive the termination or expiration of the Contract and apply to the Contractor's performance. The duration of purchase orders for recurring deliverables shall not exceed the expiration of the Contract by more than twelve months. Any purchase order terms and conditions conflicting with these Special Contract Conditions shall not become a part of the Contract.

3.5 Travel.
Travel expenses are not reimbursable unless specifically authorized by the Customer in writing and may be reimbursed only in accordance with section 112.061, F.S.

3.6 Annual Appropriation.
Pursuant to section 287.0582, F.S., if the Contract binds the State of Florida or an agency for the purchase of services or tangible personal property for a period in excess of one fiscal year, the State of Florida's performance and obligation to pay under the Contract is contingent upon an annual appropriation by the Legislature.

3.7 Transaction Fees.
The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system pursuant to section 287.057(22), F.S. All payments issued by Customers to registered Vendors for purchases of commodities or contractual services will be assessed Transaction Fees as prescribed by rule 60A-1.031, F.A.C., or as may otherwise be established by law. Vendors must pay the Transaction Fees and agree to automatic deduction of the Transaction Fees when automatic deduction becomes available. Vendors will submit any monthly reports required pursuant to the rule. All such reports and payments will be subject to audit. Failure to comply with the payment of the Transaction Fees or reporting of transactions will constitute grounds for declaring the Vendor in default and subject the Vendor to exclusion from business with the State of Florida.

3.8 Taxes.
Taxes, customs, and tariffs on commodities or contractual services purchased under the Contract will not be assessed against the Customer or Department unless authorized by Florida law.

3.9 Return of Funds.
Contractor will return any overpayments due to unearned funds or funds disallowed pursuant to the terms of the Contract that were disbursed to the Contractor. The Contractor must return any overpayment within forty (40) calendar days after either discovery by the Contractor, its independent auditor, or notification by the Department or Customer of the overpayment.

SECTION 4. CONTRACT MANAGEMENT.

4.1 Composition and Priority.
The Contractor agrees to provide commodities or contractual services to the Customer as specified in the Contract. Additionally, the terms of the Contract supersede the terms of all prior agreements between the Parties on this subject matter.

4.2 Notices.
All notices required under the Contract must be delivered to the designated Contract Manager in a manner identified by the Department.

4.3 Department's Contract Manager.
The Department's Contract Manager, who is primarily responsible for the Department's oversight of the Contract, will be identified in a separate writing to the Contractor upon Contract signing in the following format:

Department's Contract Manager Name

Department's Name
Department's Physical Address
Department's Telephone #
Department's Email Address

If the Department changes the Contract Manager, the Department will notify the Contractor. Such a change does not require an amendment to the Contract.

4.4 Contractor's Contract Manager.
The Contractor's Contract Manager, who is primarily responsible for the Contractor's oversight of the Contract performance, will be identified in a separate writing to the Department upon Contract signing in the following format:

Contractor's Contract Manager Name
Contractor's Name
Contractor's Physical Address
Contractor's Telephone #
Contractor's Email Address

If the Contractor changes its Contract Manager, the Contractor will notify the Department. Such a change does not require an amendment to the Contract.

4.5 Diversity.

4.5.1 Office of Supplier Diversity.
The State of Florida supports its diverse business community by creating opportunities for woman-, veteran-, and minority-owned small business enterprises to participate in procurements and contracts. The Department encourages supplier diversity through certification of woman-, veteran-, and minority-owned small business enterprises and provides advocacy, outreach, and networking through regional business events. For additional information, please contact the Office of Supplier Diversity (OSD) at osdinfo@dms.myflorida.com.

4.5.2 Diversity Reporting.
Upon request, the Contractor will report to the Department its spend with business enterprises certified by the OSD. These reports must include the time period covered, the name and Federal Employer Identification Number of each business enterprise utilized during the period, commodities and contractual services provided by the business enterprise, and the amount paid to the business enterprise on behalf of each agency purchasing under the Contract.

4.6 RESPECT.
Subject to the agency determination provided for in section 413.036, F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES;

AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INSOFAR AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about RESPECT and the commodities or contractual services it offers is available at https://www.respectofflorida.org.

4.7 PRIDE.
Subject to the agency determination provided for in sections 287.042(1) and 946.515, F.S., the following statement applies:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INSOFAR AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the commodities or contractual services it offers is available at https://www.pride-enterprises.org.

SECTION 5. COMPLIANCE WITH LAWS.

5.1 Conduct of Business.
The Contractor must comply with all laws, rules, codes, ordinances, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and authority. For example, the Contractor must comply with section 274A of the Immigration and Nationality Act, the Americans with Disabilities Act, Health Insurance Portability and Accountability Act, if applicable, and all prohibitions against discrimination on the basis of race, religion, sex, creed, national origin, handicap, marital status, or veteran's status. The provisions of subparagraphs 287.058(1)(a)-(c), and (g), F.S., are hereby incorporated by reference.

5.2 Dispute Resolution, Governing Law, and Venue.
Any dispute concerning performance of the Contract shall be decided by the Department's designated Contract Manager, who will reduce the decision to writing and serve a copy on the Contractor. The decision of the Contract Manager shall be final and conclusive. Exhaustion of this administrative remedy is an absolute condition precedent to the Contractor's ability to pursue legal action related to the Contract or any other form of dispute resolution. The laws of the State of Florida govern the Contract. The Parties submit to the jurisdiction of the courts of the State of Florida exclusively for any legal action related to the Contract. Further, the Contractor hereby waives all privileges and rights relating to venue it may have under Chapter 47, F.S., and all such venue privileges and rights it may have under any other statute, rule, or case law, including, but not limited to, those based on convenience. The Contractor hereby submits to venue in the county chosen by the Department.

5.3 Department of State Registration.

Consistent with Title XXXVI, F.S., the Contractor and any subcontractors that assert status, other than a sole proprietor, must provide the Department with conclusive evidence of a certificate of status, not subject to qualification, if a Florida business entity, or of a certificate of authorization if a foreign business entity.

5.4 Suspended, Convicted, and Discriminatory Vendor Lists.
In accordance with sections 287.042, 287.133, and 287.134, F.S., an entity or affiliate who is on the Suspended Vendor List, Convicted Vendor List, or Discriminatory Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Contract. The Contractor must notify the Department if it or any of its suppliers, subcontractors, or consultants have been placed on the Suspended Vendor List, Convicted Vendor List, or Discriminatory Vendor List during the term of the Contract.

5.5 Scrutinized Companies - Termination by the Department.
The Department may, at its option, terminate the Contract if the Contractor is found to have submitted a false certification as provided under section 287.135(5), F.S., or been placed on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or been engaged in business operations in Cuba or Syria, or to have been placed on the Scrutinized Companies that Boycott Israel List or is engaged in a boycott of Israel.

5.6 Cooperation with Inspector General and Records Retention.
Pursuant to section 20.055(5), F.S., the Contractor understands and will comply with its duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing. Upon request of the Inspector General or any other authorized State official, the Contractor must provide any information the Inspector General deems relevant to the Contractor's integrity or responsibility. Such information may include, but will not be limited to, the Contractor's business or financial records, documents, or files of any type or form that refer to or relate to the Contract. The Contractor will retain such records for the longer of five years after the expiration of the Contract, or the period required by the General Records Schedules maintained by the Florida Department of State, at the Department of State’s Records Management website. The Contractor agrees to reimburse the State of Florida for the reasonable costs of investigation incurred by the Inspector General or other authorized State of Florida official for investigations of the Contractor's compliance with the terms of this or any other agreement between the Contractor and the State of Florida which results in the suspension or debarment of the Contractor. Such costs will include but will not be limited to: salaries of investigators, including overtime; travel and lodging expenses; and expert witness and documentary fees. The Contractor agrees to impose the same obligations to cooperate with the Inspector General and retain records on any subcontractors used to provide goods or services under the Contract.

SECTION 6. MISCELLANEOUS.

6.1 Subcontractors.
The Contractor will not subcontract any work under the Contract without prior written consent of the Department. The Contractor is fully responsible for satisfactory completion of all its subcontracted work. The Department supports diversity in its procurements and contracts, and requests that the Contractor offer subcontracting opportunities to certified woman-, veteran-, and minority-owned small businesses. The

Contractor may contact the OSD at osdhelp@dms.myflorida.com for information on certified small business enterprises available for subcontracting opportunities.

6.2 Assignment.
The Contractor will not sell, assign, or transfer any of its rights, duties, or obligations under the Contract without the prior written consent of the Department. However, the Contractor may waive its right to receive payment and assign same upon notice to the Department. In the event of any assignment, the Contractor remains responsible for performance of the Contract, unless such responsibility is expressly waived by the Department. The Department may assign the Contract with prior written notice to the Contractor.

6.3 Independent Contractor.
The Contractor and its employees, agents, representatives, and subcontractors are independent contractors and not employees or agents of the State of Florida and are not entitled to State of Florida benefits. The Department and Customer will not be bound by any acts or conduct of the Contractor or its employees, agents, representatives, or subcontractors. The Contractor agrees to include this provision in all its subcontracts under the Contract.

6.4 Inspection and Acceptance of Commodities.

6.4.1 Risk of Loss.
Matters of inspection and acceptance are addressed in section 215.422, F.S. Until acceptance, risk of loss or damage will remain with the Contractor. The Contractor will be responsible for filing, processing, and collecting all damage claims. To assist the Contractor with damage claims, the Customer will: record any evidence of visible damage on all copies of the delivering carrier's bill of lading; report damages to the carrier and the Contractor; and provide the Contractor with a copy of the carrier's bill of lading and damage inspection report.

6.4.2 Rejected Commodities.
When a Customer rejects a commodity, Contractor will remove the commodity from the premises within ten (10) calendar days after notification of rejection, and the risk of loss will remain with the Contractor. Commodities not removed by the Contractor within ten (10) calendar days will be deemed abandoned by the Contractor, and the Customer will have the right to dispose of such commodities. Contractor will reimburse the Customer for costs and expenses incurred in storing or effecting removal or disposition of rejected commodities.

6.5 Safety Standards.
Performance of the Contract for all commodities or contractual services must comply with requirements of the Occupational Safety and Health Act and other applicable State of Florida and federal requirements.

6.6 Ombudsman.
A Vendor Ombudsman has been established within the Department of Financial Services. The duties of this office are found in section 215.422, F.S., which include disseminating information relative to prompt payment and assisting contractors in receiving their payments in a timely manner from a Customer. The Vendor Ombudsman may be contacted at (850) 413-5516.

6.7 Time is of the Essence.
Time is of the essence regarding every obligation of the Contractor under the Contract. Each obligation is deemed material, and a breach of any such obligation (including a breach resulting from untimely performance) is a material breach.

6.8 Waiver.
The delay or failure by the Department or the Customer to exercise or enforce any rights under the Contract will not constitute waiver of such rights.

6.9 Modification and Severability.
The Contract may only be modified by written agreement between the Department and the Contractor. Should a court determine any provision of the Contract is invalid, the remaining provisions will not be affected, and the rights and obligations of the Parties will be construed and enforced as if the Contract did not contain the provision held invalid.

6.10 Cooperative Purchasing.
Pursuant to their own governing laws, and subject to the agreement of the Contractor, governmental entities that are not Customers may make purchases under the terms and conditions contained herein, if agreed to by Contractor. Such purchases are independent of the Contract between the Department and the Contractor, and the Department is not a party to these transactions. Agencies seeking to make purchases under this Contract are required to follow the requirements of Rule 60A-1.045(5), F.A.C.

SECTION 7. LIABILITY AND INSURANCE.

7.1 Workers' Compensation Insurance.
The Contractor shall maintain workers' compensation insurance as required under the Florida Workers' Compensation Law or the workers' compensation law of another jurisdiction where applicable. The Contractor must require all subcontractors to similarly provide workers' compensation insurance for all of the latter's employees. In the event work is being performed by the Contractor under the Contract and any class of employees performing the work is not protected under Workers' Compensation statutes, the Contractor must provide, and cause each subcontractor to provide, adequate insurance satisfactory to the Department, for the protection of employees not otherwise protected.

7.2 General Liability Insurance.
The Contractor must secure and maintain Commercial General Liability Insurance, including bodily injury, property damage, products, personal and advertising injury, and completed operations. This insurance must provide coverage for all claims that may arise from performance of the Contract or completed operations, whether by the Contractor or anyone directly or indirectly employed by the Contractor. Such insurance must include the State of Florida as an additional insured for the entire length of the resulting contract. The Contractor is responsible for determining the minimum limits of liability necessary to provide reasonable financial protections to the Contractor and the State of Florida under the resulting contract.

7.3 Florida Authorized Insurers.

All insurance shall be with insurers authorized and eligible to transact the applicable line of insurance business in the State of Florida. The Contractor shall provide Certification(s) of Insurance evidencing that all appropriate coverage is in place and showing the Department to be an additional insured.

7.4 Performance Bond.
Unless otherwise prohibited by law, the Department may require the Contractor to furnish, without additional cost to the Department, a performance bond or irrevocable letter of credit or other form of security for the satisfactory performance of work hereunder. The Department shall determine the type and amount of security.

7.5 Indemnification.
To the extent permitted by Florida law, the Contractor agrees to indemnify, defend, and hold the Customer and the State of Florida, its officers, employees, and agents harmless from all fines, claims, assessments, suits, judgments, or damages, including consequential, special, indirect, and punitive damages, including court costs and attorney's fees, arising from or relating to violation or infringement of a trademark, copyright, patent, trade secret, or intellectual property right or out of any acts, actions, breaches, neglect, or omissions of the Contractor, its employees, agents, subcontractors, assignees, or delegates related to the Contract, as well as for any determination arising out of or related to the Contract that the Contractor or Contractor's employees, agents, subcontractors, assignees, or delegates are not independent contractors in relation to the Customer. The Contract does not constitute a waiver of sovereign immunity or consent by the Customer or the State of Florida or its subdivisions to suit by third parties. Without limiting this indemnification, the Customer may provide the Contractor (1) written notice of any action or threatened action, (2) the opportunity to take over and settle or defend any such action at Contractor's sole expense, and (3) assistance in defending the action at Contractor's sole expense.

7.6 Limitation of Liability.
Unless otherwise specifically enumerated in the Contract or in the purchase order, neither the Department nor the Customer shall be liable for special, indirect, punitive, or consequential damages, including lost data or records (unless the Contract or purchase order requires the Contractor to back-up data or records), even if the Department or Customer has been advised that such damages are possible. Neither the Department nor the Customer shall be liable for lost profits, lost revenue, or lost institutional operating savings. The Department or Customer may, in addition to other remedies available to them at law or equity and upon notice to the Contractor, retain such monies from amounts due Contractor as may be necessary to satisfy any claim for damages, penalties, costs, and the like asserted by or against them. The State may set off any liability or other obligation of the Contractor or its affiliates to the State against any payments due the Contractor under any contract with the State.

SECTION 8. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY.

8.1 Public Records.

8.1.1 Termination of Contract.

The Department may terminate the Contract for refusal by the Contractor to comply with this section by not allowing access to all public records, as defined in Chapter 119, F. S., made or received by the Contractor in conjunction with the Contract.

8.1.2 Statutory Notice.
Pursuant to section 119.0701(2)(a), F.S., for contracts for services with a contractor acting on behalf of a public agency, as defined in section 119.011(2), F.S., the following applies:

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT THE TELEPHONE NUMBER, EMAIL ADDRESS, AND MAILING ADDRESS PROVIDED IN THE RESULTING CONTRACT OR PURCHASE ORDER.

Pursuant to section 119.0701(2)(b), F.S., for contracts for services with a contractor acting on behalf of a public agency as defined in section 119.011(2), F.S., the Contractor shall:

(a) Keep and maintain public records required by the public agency to perform the service.
(b) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.
(c) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the Contract term and following the completion of the Contract if the Contractor does not transfer the records to the public agency.
(d) Upon completion of the Contract, transfer, at no cost, to the public agency all public records in possession of the Contractor or keep and maintain public records required by the public agency to perform the service. If the Contractor transfers all public records to the public agency upon completion of the Contract, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the Contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the public agency, upon request from the public agency's custodian of public records, in a format that is compatible with the information technology systems of the public agency.

8.2 Protection of Trade Secrets or Otherwise Confidential Information.

8.2.1 Contractor Designation of Trade Secrets or Otherwise Confidential Information.
If the Contractor considers any portion of materials to be trade secret under section 688.002 or 812.081, F.S., or otherwise confidential under Florida or federal law, the Contractor must clearly designate that portion of the materials as trade secret or otherwise confidential when submitted to the Department. The Contractor will be

responsible for responding to and resolving all claims for access to Contract-related materials it has designated trade secret or otherwise confidential.

8.2.2 Public Records Requests.
If the Department receives a public records request for materials designated by the Contractor as trade secret or otherwise confidential under Florida or federal law, the Contractor will be responsible for taking the appropriate legal action in response to the request. If the Contractor fails to take appropriate and timely action to protect the materials designated as trade secret or otherwise confidential, the Department will provide the materials to the requester.

8.2.3 Indemnification Related to Confidentiality of Materials.
The Contractor will protect, defend, indemnify, and hold harmless the Department for claims, costs, fines, and attorney's fees arising from or relating to its designation of materials as trade secret or otherwise confidential.

8.3 Document Management.
The Contractor must retain sufficient documentation to substantiate claims for payment under the Contract and all other records, electronic files, papers, and documents that were made in relation to this Contract. The Contractor must retain all documents related to the Contract for five (5) years after expiration of the Contract or, if longer, the period required by the General Records Schedules maintained by the Florida Department of State available at the Department of State's Records Management website.

8.4 Intellectual Property.

8.4.1 Ownership.
Unless specifically addressed otherwise in the Contract, the State of Florida shall be the owner of all intellectual property rights to all property created or developed in connection with the Contract.

8.4.2 Patentable Inventions or Discoveries.
Any inventions or discoveries developed in the course, or as a result, of services in connection with the Contract that are patentable pursuant to 35 U.S.C. § 101 are the sole property of the State of Florida. Contractor must inform the Customer of any inventions or discoveries developed or made through performance of the Contract, and such inventions or discoveries will be referred to the Florida Department of State for a determination on whether patent protection will be sought. The State of Florida will be the sole owner of all patents resulting from any invention or discovery made through performance of the Contract.

8.4.3 Copyrightable Works.
Contractor must notify the Department or State of Florida of any publications, artwork, or other copyrightable works developed in connection with the Contract. All copyrights created or developed through performance of the Contract are owned solely by the State of Florida.

SECTION 9. DATA SECURITY.

The Contractor will maintain the security of State of Florida data including, but not limited to, maintaining a secure area around any displayed visible data and ensuring data is stored and secured when not in use. The Contractor and subcontractors will not perform any of the services from outside of the United States, and the Contractor will not allow any State of Florida data to be sent by any medium, transmitted, or accessed outside the United States due to Contractor's action or inaction. In the event of a security breach involving State of Florida data, the Contractor shall give notice to the Customer and the Department within one business day. "Security breach" for purposes of this section will refer to a confirmed event that compromises the confidentiality, integrity, or availability of data. Once a data breach has been contained, the Contractor must provide the Department with a post-incident report documenting all containment, eradication, and recovery measures taken. The Department reserves the right in its sole discretion to enlist a third party to audit Contractor's findings and produce an independent report, and the Contractor will fully cooperate with the third party. The Contractor will also comply with all HIPAA requirements and any other state and federal rules and regulations regarding security of information.

SECTION 10. GRATUITIES, LOBBYING, AND COMMUNICATIONS.

10.1 Gratuities.
The Contractor will not, in connection with this Contract, directly or indirectly (1) offer, give, or agree to give anything of value to anyone as consideration for any State of Florida officer's or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State of Florida officer or employee.

10.2 Lobbying.
In accordance with sections 11.062 and 216.347, F.S., Contract funds are not to be used for the purpose of lobbying the Legislature, the judicial branch, or the Department. Pursuant to section 287.058(6), F.S., the Contract does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Contract after the Contract is executed and during the Contract term.

10.3 Communications.

10.3.1 Contractor Communication or Disclosure.
The Contractor shall not make any public statements, press releases, publicity releases, or other similar communications concerning the Contract or its subject matter or otherwise disclose or permit to be disclosed any of the data or other information obtained or furnished in compliance with the Contract, without first notifying the Customer's Contract Manager and securing the Customer's prior written consent.

10.3.2 Use of Customer Statements.
The Contractor shall not use any statement attributable to the Customer or its employees for the Contractor's promotions, press releases, publicity releases, marketing, corporate communications, or other similar communications, without first notifying the Customer's Contract Manager and securing the Customer's prior written consent.

SECTION 11. CONTRACT MONITORING.

11.1 Performance Standards.
The Contractor agrees to perform all tasks and provide deliverables as set forth in the Contract. The Department and the Customer will be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof.

11.2 Performance Deficiencies and Financial Consequences of Non-Performance.

11.2.1 Proposal of Corrective Action Plan.
In addition to the processes set forth in the Contract (e.g., service level agreements), if the Department or Customer determines that there is a performance deficiency that requires correction by the Contractor, then the Department or Customer will notify the Contractor. The correction must be made within a time-frame specified by the Department or Customer. The Contractor must provide the Department or Customer with a corrective action plan describing how the Contractor will address all performance deficiencies identified by the Department or Customer.

11.2.2 Retainage for Unacceptable Corrective Action Plan or Plan Failure.
If the corrective action plan is unacceptable to the Department or Customer, or implementation of the plan fails to remedy the performance deficiencies, the Department or Customer will retain ten percent (10%) of the total invoice amount. The retainage will be withheld until the Contractor resolves the performance deficiencies. If the performance deficiencies are resolved, the Contractor may invoice the Department or Customer for the retained amount. If the Contractor fails to resolve the performance deficiencies, the retained amount will be forfeited to compensate the Department or Customer for the performance deficiencies.

11.3 Performance Delay.

11.3.1 Notification.
The Contractor will promptly notify the Department or Customer upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion (or delivery) of any commodity or contractual service. The Contractor will use commercially reasonable efforts to avoid or minimize any delays in performance and will inform the Department or the Customer of the steps the Contractor is taking or will take to do so, and the projected actual completion (or delivery) time. If the Contractor believes a delay in performance by the Department or the Customer has caused or will cause the Contractor to be unable to perform its obligations on time, the Contractor will promptly so notify the Department and use commercially reasonable efforts to perform its obligations on time notwithstanding the Department’s delay.

11.3.2 Liquidated Damages.
The Contractor acknowledges that delayed performance will damage the DepartmentCustomer, but by their nature such damages are difficult to ascertain. Accordingly, the liquidated damages provisions stated in the Contract documents will apply. Liquidated damages are not intended to be a penalty and are solely intended to compensate for damages.

11.4 Force Majeure, Notice of Delay, and No Damages for Delay.

The Contractor will not be responsible for delay resulting from its failure to perform if neither the fault nor the negligence of the Contractor or its employees or agents contributed to the delay, and the delay is due directly to fire, explosion, earthquake, windstorm, flood, radioactive or toxic chemical hazard, war, military hostilities, terrorism, civil emergency, embargo, riot, strike, violent civil unrest, or other similar cause wholly beyond the Contractor's reasonable control, or for any of the foregoing that affect subcontractors or suppliers if no alternate source of supply is available to the Contractor. The foregoing does not excuse delay which could have been avoided if the Contractor implemented any risk mitigation required by the Contract. In case of any delay the Contractor believes is excusable, the Contractor will notify the Department in writing of the delay or potential delay and describe the cause of the delay either (1) within ten (10) calendar days after the cause that created or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result, or (2) if delay is not reasonably foreseeable, within five (5) calendar days after the date the Contractor first had reason to believe that a delay could result. The foregoing will constitute the Contractor's sole remedy or excuse with respect to delay. Providing notice in strict accordance with this paragraph is a condition precedent to such remedy. No claim for damages will be asserted by the Contractor. The Contractor will not be entitled to an increase in the Contract price or payment of any kind from the Department for direct, indirect, consequential, impact or other costs, expenses or damages, including but not limited to costs of acceleration or inefficiency, arising because of delay, disruption, interference, or hindrance from any cause whatsoever. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this paragraph, after the causes have ceased to exist the Contractor will perform at no increased cost, unless the Department determines, in its sole discretion, that the delay will significantly impair the value of the Contract to the State of Florida or to Customers, in which case the Department may (1) accept allocated performance or deliveries from the Contractor, provided that the Contractor grants preferential treatment to Customers and the Department with respect to commodities or contractual services subjected to allocation, or (2) purchase from other sources (without recourse to and by the Contractor for the related costs and expenses) to replace all or part of the commodity or contractual services that are the subject of the delay, which purchases may be deducted from the Contract quantity, or (3) terminate the Contract in whole or in part.

SECTION 12. CONTRACT AUDITS.

12.1 Performance or Compliance Audits.
The Department may conduct or have conducted performance and/or compliance audits of the Contractor and subcontractors as determined by the Department. The Department may conduct an audit and review all the Contractor's and subcontractors' data and records that directly relate to the Contract. To the extent necessary to verify the Contractor's fees and claims for payment under the Contract, the Contractor's agreements or contracts with subcontractors, partners, or agents of the Contractor, pertaining to the Contract, may be inspected by the Department upon fifteen (15) calendar days' notice, during normal working hours and in accordance with the Contractor's facility access procedures where facility access is required. Release statements from its subcontractors, partners, or agents are not required for the Department or its designee to conduct compliance and performance audits on any of the Contractor's contracts relating to this Contract. The Inspector General, in accordance with section 5.6, the State of Florida's Chief Financial Officer, the Office of the Auditor General also have authority to perform audits and inspections.

12.2 Payment Audit.
Records of costs incurred under terms of the Contract will be maintained in accordance with section 8.3 of these Special Contract Conditions. Records of costs incurred will include the Contractor's general accounting records, together with supporting documents and records of the Contractor and all subcontractors performing work, and all other records of the Contractor and subcontractors considered necessary by the Department, the State of Florida's Chief Financial Officer, or the Office of the Auditor General.

SECTION 13. BACKGROUND SCREENING AND SECURITY.

13.1 Background Check.
The Department or Customer may require the Contractor to conduct background checks of its employees, agents, representatives, and subcontractors as directed by the Department or Customer. The cost of the background checks will be borne by the Contractor. The Department or Customer may require the Contractor to exclude the Contractor's employees, agents, representatives, or subcontractors based on the background check results. In addition, the Contractor must ensure that all persons have a responsibility to self-report to the Contractor within three (3) calendar days any arrest for any disqualifying offense. The Contractor must notify the Contract Manager within twenty-four (24) hours of all details concerning any reported arrest. Upon the request of the Department or Customer, the Contractor will re-screen any of its employees, agents, representatives, and subcontractors during the term of the Contract.

13.2 E-Verify.
The Contractor must use the U.S. Department of Homeland Security's E-Verify system to verify the employment eligibility of all new employees hired during the term of the Contract for the services specified in the Contract. The Contractor must also include a requirement in subcontracts that the subcontractor must utilize the E-Verify system to verify the employment eligibility of all new employees hired by the subcontractor during the Contract term. In order to implement this provision, the Contractor must provide a copy of its DHS Memorandum of Understanding (MOU) to the Contract Manager within five (5) calendar days of Contract execution. If the Contractor is not enrolled in DHS E-Verify System, it will do so within five (5) calendar days of notice of Contract award and provide the Contract Manager a copy of its MOU within five (5) calendar days of Contract execution. The link to E-Verify is https://www.uscis.gov/e-verify. Upon each Contractor or subcontractor new hire, the Contractor must provide a statement within five (5) calendar days to the Contract Manager identifying the new hire with its E-Verify case number.

13.3 Disqualifying Offenses.
If at any time it is determined that a person has been found guilty of a misdemeanor or felony offense as a result of a trial or has entered a plea of guilty or nolo contendere, regardless of whether adjudication was withheld, within the last six (6) years from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, the Contractor is required to immediately remove that person from any position with access to State of Florida data or directly performing services under the Contract. The disqualifying offenses are as follows:

(a) Computer related crimes;
(b) Information technology crimes;

(c) Fraudulent practices;
(d) False pretenses;
(e) Frauds;
(f) Credit card crimes;
(g) Forgery;
(h) Counterfeiting;
(i) Violations involving checks or drafts;
(j) Misuse of medical or personnel records; and
(k) Felony theft.

13.4 Confidentiality.
The Contractor must maintain confidentiality of all confidential data, files, and records related to the commodities or contractual services provided pursuant to the Contract and must comply with all state and federal laws, including, but not limited to sections 381.004, 384.29, 392.65, and 456.057, F.S. The Contractor's confidentiality procedures must be consistent with the most recent version of the Department security policies, protocols, and procedures. The Contractor must also comply with any applicable professional standards with respect to confidentiality of information.

SECTION 14. WARRANTY OF CONTRACTOR'S ABILITY TO PERFORM.

The Contractor warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Contract obligations. The Contractor warrants that neither it nor any affiliate is currently on the Suspended Vendor List, Convicted Vendor List, or the Discriminatory Vendor List, or on any similar list maintained by any other state or the federal government. The Contractor shall immediately notify the Department in writing if its ability to perform is compromised in any manner during the term of the Contract.

Contract #: AR3116

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

Visionary Integration Professionals, LLC
Name

80 Iron Point Cir. #100
Street Address

Folsom	CA	95630
City	*State*	*Zip*

Vendor # VC226516 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact *Name:* Steve Carpenter *Phone Number:* 916-985-9625 *Email:* scarpenter@trustvip.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Monday, March 11, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs, etc.

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Stephen A. Carpenter 03.07.2019
Contractor's signature Date

STEPHEN A. CARPENTER
Type or Print Name and Title

CHIEF ADMINISTRATIVE OFFICER.

DIVISION OF PURCHASING

Christopher Hughes
Christopher Hughes (Mar 8, 2019)
Director, Division of Purchasing

Mar 8, 2019
Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate.

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) 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 (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing

Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the

solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in

performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and

reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000
Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states);

a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this

authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its

assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the

Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection

with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity,

including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to

NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data

within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO

ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	X			Multi-tenant SaaS (Public) Cloud or a Single-tenant (Private) SaaS Cloud. VIP is also offering SaaS with FedRAMP Accreditation multi-tenant or single-tenant.

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Cloud Service Model: Software as a Service (SaaS)

Contractor: **Visionary Integration Professionals**

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

SaaS Minimum Discount % Off

Description	Discount
SaaS Minimum Discount %*	15.00%

*(applies to all OEM's offered within this SaaS model)

Additional Value Added Services

Item Description	Onsite Hourly Rate NVP Price	Onsite Hourly Rate Catalog Price	Remote Hourly Rate NVP Price	Remote Hourly Rate Catalog Price
Maintenance Services	N/A	N/A	N/A	N/A
Professional Services	N/A	N/A	N/A	N/A
Deployment Services	N/A	N/A	N/A	N/A
Integration Services)	N/A	N/A	N/A	N/A
Consulting/Advisory Services	N/A	N/A	N/A	N/A
Architectural Design Services	N/A	N/A	N/A	N/A
Statement of Work Services	N/A	N/A	N/A	N/A
Partner Services	N/A	N/A	N/A	N/A
Training Deployment Services	N/A	N/A	N/A	N/A
Technical Writer	$ 115.00	$ 135.29	$ 90.00	$ 105.88
Application Architect	$ 205.00	$ 241.18	$ 180.00	$ 211.76
Sr. Application Architect	$ 230.00	$ 270.59	$ 205.00	$ 241.18
Application Developer	$ 155.00	$ 182.35	$ 130.00	$ 152.94
Sr. Application Developer	$ 185.00	$ 217.65	$ 160.00	$ 188.24
Business Systems Analyst	$ 150.00	$ 176.47	$ 125.00	$ 147.06
Sr. Business Systems Analyst	$ 175.00	$ 205.88	$ 150.00	$ 176.47
Director	$ 215.00	$ 252.94	$ 190.00	$ 223.53
Sr. Director	$ 255.00	$ 300.00	$ 230.00	$ 270.59
Instructional Designer	$ 115.00	$ 135.29	$ 90.00	$ 105.88
Sr. Instructional Designer	$ 150.00	$ 176.47	$ 125.00	$ 147.06
Instructional Technologist	$ 150.00	$ 176.47	$ 125.00	$ 147.06
Sr. Instructional Technologist	$ 200.00	$ 235.29	$ 175.00	$ 205.88
Knowledge Management Consultant	$ 150.00	$ 176.47	$ 125.00	$ 147.06
Sr. Knowledge Management Consult	$ 175.00	$ 205.88	$ 150.00	$ 176.47
Project Manager	$ 175.00	$ 205.88	$ 150.00	$ 176.47
Sr. Project Manager	$ 205.00	$ 241.18	$ 180.00	$ 211.76
QA/QC Specialist	$ 150.00	$ 176.47	$ 125.00	$ 147.06
Sr. QA/QC Specialist	$ 175.00	$ 205.88	$ 150.00	$ 176.47
Trainer	$ 135.00	$ 158.82	$ 110.00	$ 129.41
Strategic Implementation Consultan	$ 275.00	$ 323.53	$ 250.00	$ 294.12
Sr. Strategic Implementation Consul	$ 300.00	$ 352.94	$ 275.00	$ 323.53
Web Designer	$ 125.00	$ 147.06	$ 100.00	$ 117.65
Sr. Web Designer	$ 150.00	$ 176.47	$ 125.00	$ 147.06
System Administrator	$ 175.00	$ 205.88	$ 150.00	$ 176.47

Attachment C - Pricing Discounts and Schedule

Cloud Service Model: Software as a Service (SaaS)

Contractor:	**Visionary Integration Professionals**			
Database Administrator	$ 190.00	$ 223.53	$ 165.00	$ 194.12

	Deliverable Rates	
	NVP Price	**Catalog Price**
N/A*	N/A*	N/A*

*VIP Provided hourly rates as required. Deliverables-based pricing available upon request.

Proposal To: State of Utah in Conjunction with NASPO Value Point

Request for Proposal (RFP) Number SK18008
Cloud Solutions

Consolidated Redacted Proposal

Proposal from:
Visionary Integration Professionals, LLC

Point of Contact:
Steve Carpenter
Vice President, Administration

Address:
80 Iron Point Circle, Suite 100
Folsom, CA 95630
Phone: (916) 985-9625
Email: SCarpenter@trustvip.com

1 Executive Summary

The one to three page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.2 of the RFP.

The State of Utah, Division of Purchasing (Lead State) is requesting proposals for cloud solutions in furtherance of the NASPO ValuePoint Cooperative Purchasing Program. The purpose of this Request for Proposals (RFP) is to establish Master Agreements with qualified Offerors to provide services related to cloud solutions for all Participating Entities.

VIP is pleased to present our response to RFP SK18008 for NASPO ValuePoint Master Agreement for Cloud Solutions. VIP is an information technology and management consulting firm providing mission support to government agencies nationwide; delivering a full range of cloud solutions and services. Our management consulting and technology solution capabilities provide the visibility, proven execution, and agility to accelerate strategic support and achieve measurable results.

VIP is proposing Software as a Service (SaaS) cloud solutions and value-added services. VIP's SaaS offerings include the award-winning Meridian Learning Management System (Meridian LMS ™) platform. Meridian LMS supports learning and knowledge (enterprise training and learning management) initiatives in many of the world's leading organizations and government agencies.

VIP HIGHLIGHTS

- 1,200+ Commercial & Public-Sector Clients Nationwide
- 450+ Experienced Staff Members
- Appraised at a CMMI Level 3
- Industry-leading alliances and certifications
- 22 years' experience creating a strategic approach to achieve measurable results

With over 22 years supporting government agencies on some of the largest local, state, and federal government projects, VIP is ideally positioned to support this NASPO ValuePoint Contract. We have a successful track record supporting agencies on similar initiatives and providing cloud solution subject matter expertise. VIP's mission is commitment to quality, delivery and the successful completion of all projects to our clients' satisfaction. As you review our proposal, please note the reasons why VIP is an excellent choice to support this effort:

- NASPO ValuePoint, the Lead State, and participating States receive a responsive and reliable vendor with extensive experience providing cloud solutions and services nationwide. VIP meets the administrative and technical requirements to support this contract and has demonstrated the ability to successfully deliver results to meet our client's unique needs for more than two decades. VIP did not identify any requirements in this RFP that cannot be met by VIP.
- VIP has deep knowledge of the market and changes that have impacted cloud solutions in recent years. We have been working with government agencies nationwide since our inception, and we have successfully secured leveraged procurement agreements (LPAs) in over a dozen States. We look forward to being another proven vendor available for participating states to secure cloud solutions and services.

- VIP has the agility of a small business with the mature infrastructure and proven processes of a large company. We deploy the same level of expertise as larger providers, but our streamlined business model allows us to offer more value and a higher return on investment while meeting our client's unique needs.
- We have served over 1,200 customers nationwide and hold procurement vehicles with support in multiple states similar to this Master Agreement. Clients include local, state, and federal government agencies nationwide. The below figure provides a sample of contracts and vehicles we hold in multiple states as well as several nationwide contracts and procurement vehicles.

Figure 1 - VIP's Contracts / Procurement Vehicles

- We have a proven track record and reputation of working with numerous organizations to establish and leverage master contract vehicles in support of mission-critical projects. We continuously build our cloud solutions practice with experts who bring extensive cloud and government experience in different States. As highlighted by our customers, our cloud solutions offerings provide NASPO ValuePoint with industry-leading SaaS solutions, highly competitive prices, and exceptional overall value.

Our proposal blends relevant experience and expertise with industry-leading SaaS offerings and a competitive pricing model to provide NASPO with a high-value and low-risk vendor for cloud solutions. Our staff have the demonstrated ability to roll up their sleeves and provide leadership across multiple industries and geographies. VIP's unique skills and experience provides the consistent, reliable, long-term coverage this contract requires. We look forward to the opportunity of supporting the Lead State in furtherance of the NASPO ValuePoint Cooperative Purchasing Program via the Cloud Solutions Master Agreement.

Please see the table below for major features of our proposal.

Table 1: VIP Proposal Feature Highlights

VIP Cloud Solutions Proposal Sections	
Section 1 – Executive Summary	This section provides the Lead State with a description of VIP's proposal including highlights of major features included in our response.
Section 2 – Cover Letter	This section is VIP's Cover letter containing required information per the RFP.
Section 3 – Mandatory Minimums Response	This section contains point-by-point response to mandatory minimum requirements from Section 5 of the RFP. Our response includes acknowledgment and agreement with general requirements and our sample Service Level Agreement.
Section 4 – Business Information	This section contains point-by-point response to items described in Section 6 of the RFP. Our response includes: Business profile, Scope of Experience, VIP Financial Information, VIP General Information, VIP Billing & Pricing practices, and VIP Best Practices for cloud-delivered services.
Section 5 – Organization and Staffing	This Section includes information on our Contract Manager, the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah.
Section 6 – Technical Response	This section includes VIP's technical narrative and response to the technical requirements contained in the RFP.
Section 7 – Redacted Proposal	This section includes redactions for confidential, protected, or proprietary information.
Section 8 – Exceptions and/or Additions to the Master Agreement Terms and Conditions	This section includes any exceptions or additions identified for the Master Agreement Terms and Conditions.
Section 9 – Cost Proposal (Attachment F)	This section includes VIP's cost proposal for SaaS and value-added services. Please note, per RFP requirements, the Cost proposal is submitted separately from the technical proposal.
Section 10 – Cloud Offerings Search Tool (Attachment I)	This Section constitutes VIP's response to the Attachment I Cloud Offerings Search Tool as described in RFP Attachment A Section 45.

3 Mandatory Minimums

This document should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Cover Letter) and 5.2 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses to each mandatory minimum requirement. If a mandatory minimum requirement is not applicable to an Offeror's Solution then the Offeror must explain why the mandatory minimum requirement is not applicable.

3.1 (M) GENERAL REQUIREMENTS

3.1.1 Usage Report Administrator

5.3.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

VIP agrees that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described in the Master Agreement Terms and Conditions, and Participating Addendums if applicable.

3.1.2 Cooperating with NASPO ValuePoint and SciQuest

5.3.2 Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

VIP agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading VIP's ordering instructions, if awarded a contract.

3.1.3 CSA STAR Registry Self-Assessment

5.3.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed assessment. Offerors are encouraged to complete and submit both exhibits to Attachment B.

VIP has submitted a completed Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B for its SaaS Cloud Offerings.

VIP represents and warrants the accuracy and currency of the information on the completed assessment at the time of submission of this response.

3.1.4 Sample Service Level Agreement

5.3.4 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Provided in Document 3 Appendix A is a sample of VIP's Meridian's Multi-Tenant SaaS Service Level Agreement, which defines the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

3.1.5 Solutions & Subcategories Offered

5.3.5 Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

The following list identifies the subcategories that are being offered for our proposed Meridian Learning Management System.

- Analytics

  - Data Analytics
  - Business Intelligence
- Business Continuity/Disaster Recovery
- Cloud and Infrastructure Management Tools
- Collaboration
- Customer Relationship Management
- Data Management
- Electronic Records Management
- Human Resource
- Licensing and Registration Systems
- Meeting Planning, hosting, conferencing
- Mobile Data Management
- Security
- Workflow and Electronic Signature
- Other (identify additional sub-categories and/or descriptors)
  - Training management (classroom and virtual)
  - Learning management (classroom and virtual)
  - eCommerce
  - Social Learning and Collaboration
  - Career Development and Competency Management
  - Informal Training Management
  - On the Job Training (OJT) Management
  - External Learning Management
  - Performance Management

3.2 Recertification of Mandatory Minimums & Technical Specifications

5.4 RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS *Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal*

VIP acknowledge that if awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceed the technical capabilities discussed in its proposal

4 Business Information

This document should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.

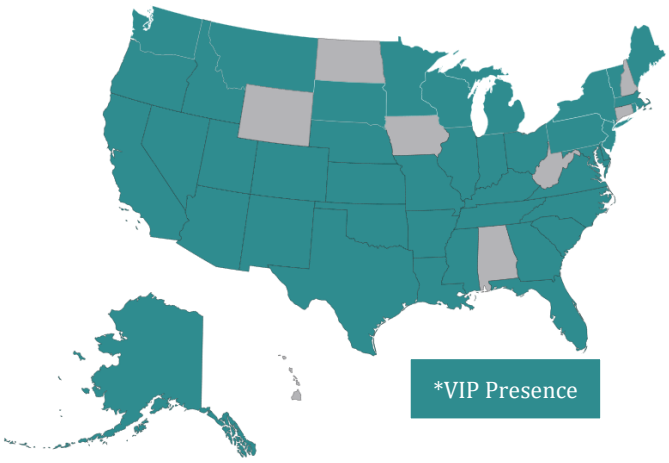
4.1 Business Profile

Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. ***Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.***

VIP's corporate credentials demonstrate our commitment to the public sector with experience serving government agencies of all shapes and sizes throughout the United States.

This extensive experience has taught us to anticipate challenges resulting from legislative changes, constituent demands, technology advancements, and economic trends; providing familiarity with current issues, trends, and trade-offs facing government organizations. We pride ourselves in cultivating a creative solution to each agency's unique mission, requirements, and issues.

Figure 1: VIP Nationwide Presence



Our success in providing cloud solutions and services in the public sector is due to our 22 years of experience that we've used to hone our ability to identify, develop and provide experienced personnel and creative, well-defined solutions. From managing tight budgets and mitigating project risks to evaluating different approaches to provide exceptional solutions and support, VIP is committed to quality delivery and successful completion of projects to client satisfaction. The following table provides the company profile details requested in the RFP.

Table 1: VIP Company Profile

VIP Company Profile	
a. Description of your company's ownership/organizational structure	VIP is a privately held limited liability company (LLC) established in 1996 and formed in Delaware. VIP has 3 primary lines of business: Commercial, State & Local Government, and Federal Government.
b. Employee size (number of employees)	Due to the nature of the consulting industry, our employee size fluctuates on a regular basis. VIP currently has over 450 experienced and knowledgeable staff serving, supporting and responding to client needs nationwide.
c. Client Base	VIP has served over 1,200 clients since our inception. Year-to-date, VIP is serving over 60 government clients,

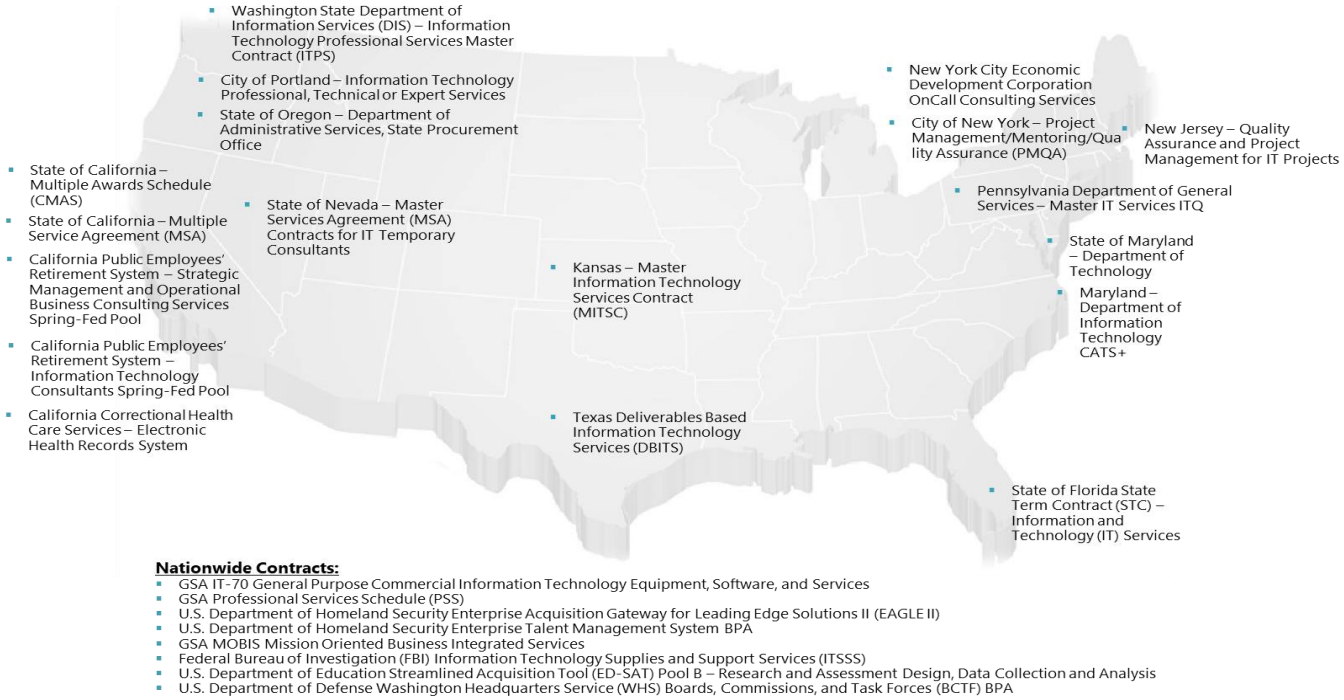
VIP Company Profile	
	many of which have multiple contracts with VIP. Our customers are spread across the United States.
d. Employee Retention	We have one of the highest retention (low turnover of employees) figures in our industry; historically, retaining over 80% of our personnel working on government contracts, in an industry that traditionally averages closer to 60%. This retention rate is based on continuing employment after a contract has ended and moving the consultant on to a new project.
e. Your client retention rate during the past 3 years	90% of our revenue year over year comes from repeat customers.
f. Description of your company's growth during the past three years.	VIP has had continued growth since our inception in 1996. We experienced 2% revenue growth between 2016 and 2017 and approximately 75% of projected 2018 revenue is already under contract, indicating additional growth will be realized in 2018. We work hard to maintain diversification with our revenue and mix across markets, solution offerings and customers. This diversification means we are not dependent on any single market, solution offering, or customer to sustain our business.
g. Demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience	VIP has over a decade providing cloud solutions for large scale projects including government. Please see Section 4.2 Scope of Experience which includes 10 of our large customers where VIP has provided cloud solutions. We have supported several of these customers dating back to the mid-2000's.

4.2 Scope of Experience

Describe in detail *the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred.*

VIP brings extensive experience with government and large consortium contracts similar to the Master Agreements sought through this RFP. With our expansive footprint across the United States, VIP provides the Lead State and Participating States with a proven vendor capable of providing the solutions and services required to support this RFP. VIP has experience in multiple participating States with first-hand knowledge of their processes, policies, and procedures. We have served over 1,200 customers nationwide and hold multiple procurement vehicles with support in multiple states similar to NASPO with federal, state and local governments nationwide. The below figure identifies vehicles we hold in multiple states as well as nationwide contracts/procurement vehicles.

Figure 2: VIP's Contracts / Procurement Vehicles



VIP has included ten (10) large contracts within the last two (2) years, which includes five (5) of our largest contracts in the last two years, under which VIP provided solutions identical or very similar to those required by this RFP. All of the contracts below are with Meridian and for Local, State, or Federal government.

Table 2: VIP's largest contracts -REDACTED

Client	Dates of Service	Approximate Dollar Value
REDACTED		

Our proposed SaaS offering is Meridian LMS. Meridian has 20+ years of proven and successful experience managing complex BPAs/IDIQs and large-scale government training programs. Meridian has proven experience encompassing complex requirements critical to the success of the client's mission. Meridian's approach embodies the key elements of program management including Governance, Management, Financial Management, and Infrastructure.

4.3 Financials

Offeror must provide audited or unaudited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement. If the minimum D&B credit rating is not applicable to an Offeror's Solution then the Offeror must explain why the minimum credit rating is not applicable. If a government entity is bidding on this RFP, a D&B credit rating and number is not required for the government entity.

VIP has included, in Appendix A of this document, unaudited financial statements per requirements of the RFP to demonstrate VIP's financial strength and stability. Additionally, VIP has included proof of its Dun and Bradstreet rating, in Appendix B of this document, with a viability score of 2-1-B which exceeds the minimum level prescribed by the RFP. VIP's D&B number is 03-694-3280. While the attached D&B report indicates Visionary Integration Professionals, LLC is a subsidiary of Visionary Integration Professionals, Inc. - the LLC is the operating entity that is financially responsible for performance of this agreement with the corporate entity merely acting as a holding company of the LLC's membership units.

Please note the financial information and D&B report are proprietary and confidential as identified on Attachment J.

4.4 General Information

4.4.1 Depth & Breadth of Solutions

6.4.1 Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace.

VIP's proposed Meridian LMS is a leading SaaS solution in the Learning Management System and eLearning technology industry. Our solution is used by organizations seeking to train employees to confirm compliance with internal or governing body audits and/or organizations to seek to drive revenue by selling training to external users (members, clients/customers, channel partners, resellers, etc.). Meridian has 350+ implementations and has provided hosting services and software-as-a-service to the federal government, state and local governments, and commercial sectors for over 20 years.

Figure 3: Sampling of Clients - REDACTED

Meridian's client base includes organizations in a variety of industries. The figure above provides a sampling of our clients across some of our target verticals.

Meridian works extensively in state and local government with implementations of the solution for:

- Commonwealth of Virginia—Enterprise
- State of Georgia—Multiple state agencies and departments
- Los Angeles County (CA)—Enterprise
- Fairfax County (VA)—Enterprise
- New York City (NY)—Multiple city agencies and departments
- Many other cities, counties, and state government agencies

4.4.2 Auditing Capabilities & Reports

6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II (SSAE 16 6/2011 or greater) compliant.

4.5 Billing & Pricing Practices

DO NOT INCLUDE YOUR PRICING CATALOG, as part of your response to this question.

4.5.1 Billing & Pricing Practices

6.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

VIP provides transparent and easy to understand pricing for Purchasing Entities. Pricing of Meridian LMS is based upon user count. Each tier of users (5,000; 10,000; etc.) has a corresponding cost. Benefits of scale apply (user costs decrease as the number of users rise). For maximum flexibility Meridian's standard payment and billing terms are often negotiable to meet client business needs. As an example, differences between internal and external users may be negotiable based on differences in usage rates. Billing for SaaS subscriptions is done on an annual basis for the upcoming 12 months. Billing for value added services is based on pricing in our cost worksheet and is defined in each participating addendum to meet our client's unique needs.

VIP looks forward to working with Purchasing Entities to continue providing transparent and easy to understand billing and pricing practices for the benefit of all parties involved.

4.5.2 Typical Cost Impacts

6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

Cost impacts for the Meridian SaaS LMS are:

- License fees by user count (annual LMS subscription fee)
- Implementation Fees—including consulting, project management, minor integrations, risk management, and other project tasks

- Value added services costs including complex integrations and product extensions, enhancements, or other support services
- Administrator Training

The risks to any given project that may impact cost are:

- Purchasing entity changes the scope of the project
- Purchasing entity changes project resource availability
- Purchasing entity changes project budget availability

These cost impact risks are mitigated through change management controls and a risk management methodology established over 22+ years of providing similar solutions and services for hundreds of government clients.

4.5.3 NIST Compliance

6.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.

Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II (SSAE 16 6/2011 or greater) compliant.

4.6 Best Practices

Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

VIP's Meridian LMS solution supports learning and knowledge initiatives in many of the world's leading organizations and government agencies. VIP and Meridian understand the importance of having the right systems in place to effectively manage talent, and how these solutions can lead to higher levels of productivity. When your people perform at their best, your company can realize tangible business results.

Meridian uses best of breed technologies from Cisco, F5, Dell, NetApp, and VMware to help us deliver a robust LMS cloud that support organizations of all sizes and in all industries. Meridian's experienced operations team manages our entire technology stack to ensure an optimal experience is delivered to our customers.

Meridian LMS offerings include the following:

- 100% Meridian Managed Environment
- State-of-the-art Facilitates & Security
- Redundant, Fault-Tolerant Power & HVAC
- Redundant Network Components and Internet Service Providers (ISPs)
- Enterprise Firewall, Intrusion Detection and Intrusion Prevention
- Real-Time Network, Security, and Availability Monitoring
- Highly Available Storage Systems
- Secure Data Backups Storage & Retention

4.6.1 Availability

Customers can access their LMS anytime, with full peace of mind. Meridian offers a standard guarantee of 99.7% uptime, which we take pride in regularly exceeding.

4.6.2 Real-Time Monitoring

Within Meridian's cloud, we track many different metrics regarding system availability and performance through our monitoring solutions to ensure service levels are achieved. Our 24x7x365 monitoring solutions provide real-time monitoring of our networks, systems, and software which allows Meridian to provide a variety of reports upon request.

4.6.3 Scalability

Meridian LMS is a multi-tiered application built upon the .NET framework and designed from the ground up with scalability in mind. Each of the application tiers can be scaled up or down to meet customer demand.

While Meridian LMS is not bandwidth intensive, the content customers make available to their users can be. It is important that content types and delivery methods are examined to ensure that they can be accessed by a customer's user base.

To help ensure Meridian LMS and any uploaded content can be accessed efficiently by users distributed across the globe, Meridian also offers Content Delivery Network (or CDN) services. The CDN utilizes caching and traffic acceleration techniques that have proven to decrease round-trips to Meridian LMS origin servers, reduce the number of ISP hops for users, increase overall download/transfer speeds, and improve overall LMS site performance.

In many cases, high levels of user concurrency will be required of the Meridian LMS due to the nature of customer's seasonal training needs. Meridian has the expertise necessary to provide our clients a secure, scalable LMS solution that will meet their needs today and as they grown in the future.

4.6.4 System Security

Meridian maintains significant real-world experience and expertise in developing secure LMS solutions for organizations of all sizes, complexity, and sophistication. We utilize some of the most advanced technology and solutions available for internet security.

4.6.4.1 Industry-Leading Data Center Facilities

Millions of users across the globe depend on Meridian solutions. Meridian hosted solutions are handled by a secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II compliant. Because of the area's strategic importance as the Eastern hub of traffic exchange to the United States, Equinix's Ashburn data center campus represents one of the largest Internet exchange points in the world. Equinix provides peering and traffic exchange services for large networks, carriers and ISPs from all over the globe.

Our operational cloud environment is located in dedicated, secure co-located, space and takes advantage of some of the industry's most advanced security, power, cooling, and emergency management technologies to provide an industry-leading 99.9999% facility uptime record. Within this environment we offer reliable infrastructure, fast connectivity, and 24x7 system/network monitoring. This state-of-the-art data center is built to ensure efficient, reliable and continuous operations—even in the event of severe natural or man-made catastrophes.

Meridian also supports clients in a wide variety of industries that choose our on-premise hosting option—each client having their own certification and accreditation processes. We have extensive experience working side-by-side with clients to deploy their learning platforms. We also have extensive experience operating within highly secure organizations and helping them prepare applications as additions to approved product lists. This includes organizations within the intelligence community, such as the US Department of Defense (DoD), the US Department of Homeland Security (DHS), as well as major pharmaceutical clients.

4.6.4.2 Physical Security

The physical security of the data center is one of our highest priorities. Physical access is tightly controlled and restricted to preauthorized personnel only. Preauthorized access is approved only for those that have an ongoing need to support Meridian hardware.

The data center utilizes an array of security equipment, techniques and procedures to control, monitor and record access to the facilities including:

- Manned by onsite security on a 24x7x365 basis
- All doors, including cages, are secured with biometric hand geometry readers
- CCTV digital camera coverage of entire center, including cages, with archival system
- A silent alarm and automatic notification of appropriate law enforcement officials protect all exterior entrances
- CCTV integrated with access control and alarm system
- Motion-detection for lighting and CCTV coverage
- All equipment checked/screened upon arrival
- Visitors are screened upon entry to verify their identity, and in shared situations, are escorted to their appropriate locations
- Shipping and receiving area walled off from co-location areas Firewalls and Intrusion Prevention

4.6.4.3 Threat Prevention

Meridian utilizes fully redundant firewalls, intrusion detection, and intrusion prevention devices from Cisco to help us protect our customer's systems from external threats and help meet ever-increasing compliance mandates. Cisco is one of the most trusted and widely-deployed providers of firewall and threat prevention technology in the world. They invest hundreds of millions of dollars in security research, employs hundreds of threat analysts, and ingest terabytes of threat data into their threat database every day. Our intrusion prevention system is integrated into redundant firewalls, switch, and router platforms, is constantly updated from Cisco's threat database, and collaborates with other key network components for maximum protection and flexibility.

Our threat prevention accurately identifies, classifies, and stops malicious traffic before it can affect underlying systems. We defend against zero-day attacks using Anomaly Detection and 6,500 stateful, vulnerability-based signatures that protect against tens of thousands of current and future exploits. We also inspect a wide variety of protocols to ensure Request for Comment (RFC) conformance and prevent hacks.

4.6.4.4 Anti-Virus

Meridian utilizes industry leading Anti-Virus solutions from McAfee to protect against system viruses, spyware, and malware. We employ centrally managed, policy-based controls to ensure all servers are protected. Policies ensure servers utilize use real-time virus scanning, perform a weekly full scan, have the latest virus scan patches, and receive the latest definitions.

4.6.4.5 Encryption

To ensure the privacy and security of your data, Meridian uses HTTPS for all communication and encrypts all inbound and outbound traffic using 128-bit and 256-bit TLS.

When data is transmitted to Meridian LMS, it first passes through the User Interface (UI) tier. Meridian LMS does not use any plug-ins that could potentially compromise security. Actions taken through the UI tier request data from, and submit data to, a dedicated Business Logic (BL) tier.

The BL tier acts as an interface between the UI tier and the database tier and maintains data integrity. It is not directly accessible via the internet and interfaces directly with the UI tier. The BL tier connects to a customer's database via a Windows service account for that specific client that only has access to that customer's data. The database tier, is located securely on a sub-network behind our firewalls and only accessible through secured connections.

Operational data stored at rest in the database, like passwords, are secured using FIPS compliant cryptography which utilizes a one-way, irreversible hashing algorithm. Personally Identifiable Information (PII) data is not required or requested by Meridian LMS, however customers can leverage custom fields to add any data they choose. Adding PII to any system should be carefully thought out and done so with care.

4.6.4.6 Patching

It is necessary to plan for security updates and revision updates to not only our LMS software but also to any of the components supporting it. All software and hardware vendors periodically release new revisions of their product so that new security holes are resolved and new features are added. The Meridian team maintains a rigorous patching process for applying and validating patches to supporting hardware, operating systems, and supporting backend applications.

Patching and system maintenance activities occur monthly and include:

- Operating System Updates – Security updates and enhancements from the OS vendors
- Firmware Updates – Firmware updates for networking and other shared hardware devices
- Backend Software Updates – Software updates for applications supporting of Meridian LMS (SQL Server, Mail Relay, SFTP, etc.)
- Meridian LMS Updates – Software code updates to Meridian LMS

4.6.4.7 Backup & Recovery

Meridian's backup process blends multiple types of backup software and hardware to ensure the reliability of our backups. These systems build redundancy to our backup plan and ensure that a recent backup is always available, in the event it's ever needed for recovery.

Meridian's backup process includes:

- Nightly Reverse Incremental Backups of all Production Virtual Machines
- Nightly Full Database Backups and 15 Minute Log Shipping

- Nightly Offsite Encrypted and Secure Transfers to a private Amazon Web Services Virtual Tape Library

As part of our backup procedures, Meridian executes a daily verification checklist. Meridian utilizes automated systems and notifications to assist in the verification of backups; however, a member of our operations team also does a manual verification each day to ensure backups are valid.

Meridian leverages the services of AWS for secure offsite backup storage. Backup data is encrypted and securely transferred from Meridian's to the US East Region and multiple availability zones on a nightly basis. Backups are stored using both S3 and Glacier Amazon services as part of the Virtual Tape Library offering.

Customer backup data is also kept for thirty (30) days onsite for quick access in the rare event that it is needed for immediate recovery.

4.6.5 Protecting Customer Data

4.6.5.1 Privacy & Data Collection

Meridian follows the minimum necessary standard in collecting and storing information needed for the operation of our software. Normal operation of Meridian LMS does not require any sensitive information such as SSN or date of birth for users. If ecommerce features are used, payment card information such as credit card numbers, are never stored by Meridian. Information such as IP address of a user accessing the system may be collected for analytical and security purposes, but not retained more than 90 days.

Meridian is Privacy Shield certified and remains committed to support privacy standards set forth in in the Generally Accepted Privacy Principles (GAPP) and EU General Data Protection Regulation (GDPR).

4.6.5.2 Access Control

Access to customer data is tightly controlled. Normal staff do not have access to customer systems or data contained within them. A small group of key operations support staff, do have access to customer data and systems as it is required for ongoing support, operation, and backup of the Meridian LMS.

There are times when elevated access as read-only (or with write-access) may be needed by another team member to maintain, troubleshoot, or resolve issues related to customer production (or lower environment) systems. If this need arises, a detailed request including the type of access and duration needed must be submitted for approval. Elevated access requests are reviewed and only approved on a need-to-have basis. Once elevated access is granted, it will be available for the time specified and only for the customer (and environments) for which it was approved.

4.6.5.3 Security Policy

Meridian recognizes technology is only part of a total security solution. Along with technology, Meridian ensures security policy, procedures, and organizational security awareness are applied in a systematic manner. Meridian conducts annual security awareness training for all staff, as well as annual review of IT security policies with key operational staff.

4.6.6 Security Testing

Meridian LMS undergoes regular security and performance testing to ensure that all modules are secure, stable and meet acceptable response times even under heavy loads. Our real-life experience

with large-scale customer, and an understanding of these tests and results all us to scale our application to meet very high customer usage requirements.

4.6.6.1 Penetration Testing

Meridian utilizes a third-party security services firm to perform an annual assessment of our information security measures and identify any security vulnerabilities. The assessment includes an external penetration (Pen) test performed by a team comprised of experienced and credentialed security engineers holding industry recognized certifications from leading institutions such as ISC2, PCI SSC, and SANS.

The Pen test is compliant with NIST Special Publication 800-115 and leverages over 60,000 tests to discover key systems, network, processes and identify application vulnerabilities in publicly accessible computer systems and network devices. It also includes:

- Full public address-space reconnaissance to identify rogue/unpublished nodes or applications.
- Manual & hybrid vulnerability tests for all externally accessible systems and services.
- Identification of weak systems or network devices on perimeter that expose the organization to hackers, malware and other threats.

Any vulnerabilities are further assessed to determine the level of risk a particular vulnerability or threat may impose to the overall environment. Meridian assesses any findings from the annual assessment and plans remediation actions based upon the severity of findings (if any).

A certification letter describing the results of Meridian's annual security assessment is available upon request.

4.6.6.2 Application Security

Meridian utilizes strict coding standards to ensure that all code is developed in the most secure manner possible and limits any potential vulnerabilities. Prior to each release, Meridian performs automated security testing to identify any vulnerabilities which may have arisen from any functionality that was newly introduced. If vulnerabilities are uncovered (and confirmed), either through code reviews or through our automated security testing they are remediated based on severity using the following guidelines:

- Critical - remediated prior to release
- High & Medium – remediated in next hotfix (if not sooner)
- Low – remediated in next version update (if not sooner)

4.6.6.3 Performance Testing

Meridian conducts internal performance testing which includes emulating normal and peak user loads on the application to evaluate how the application and the environment respond during such tests. Our performance testing includes load and stress testing, environment response times, and application profiling. Load and stress tests measure all components of a system, including the network, database(s), server(s), and computer security components.

5 Organization and Staffing

This document should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.
The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. ***The Contract Manager must have experience managing contracts for cloud solutions.***

5.1 Contract Manager

VIP is proving an experienced Contract Manager, REDACTED, as the single point of contact for management of the NASPO ValuePoint Master Agreement. REDACTED has the knowledge, experience, skills and ability to manage this contract. His experience includes managing multiple contracts for cloud solutions, including nationwide contracts. His relationships with clients and technology partner companies is a valuable asset while serving as the Contract Manager.

5.1.1 Contract Manager Contact Information

7.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

REDACTED

5.1.2 Contract Manager's Experience

7.1.2 ***Describe in detail*** *the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP.* ***Provide a detailed resume for the Contract Manager.***

5.1.2.1 Resume - REDACTED

REDACTED

5.1.3 Roles & Responsibilities of Contract Manager

7.1.3 Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

VIP provides an experienced and dedicated Contract Manager, REDACTED, who serves as the single point of contact for the NASPO ValuePoint Master Agreement. REDACTED is a certified Project Management Professional (PMP) with a broad background in government projects and has extensive experience managing contracts for cloud solutions nationwide. Our Contract Manager roles and responsibilities include, but are not limited to:

- Acting as the single point of contact for all inquiries, resource requests, issues, and more
- Acting as a point of escalation for the Lead State and other participating States
- Maintaining an effective management and communication plan for the master agreement and participating addendums
- Ensuring customer satisfaction throughout the contract term including ongoing customer feedback and performance assessments
- Reporting of sales data on a quarterly basis and utilizing the required reporting tools as specified by this master agreement

- Providing an executive summary on a quarterly basis which includes required information as specified by this master agreement
- Monitoring, maintaining, and updating VIP's cloud solution offerings
- Maintaining transparent and easy to understand billing and pricing practices

VIP presents NASPO with an effective model for managing the demand for support from participating States, adjusting as needed to the specific processes and protocols for each State. Having a single point of contact ensures the Master Agreement and the participating states have access to a representative familiar with all aspects of the contract. Additionally, REDACTED continuously monitors contract performance against predefined performance metrics, providing a proactive approach to customer service.

Our management approach provides clear lines of communication. REDACTED is the primary contact for this NASPO contract and is the single point of contact for all inquiries, resource requests, issues and provides escalation if needed.

6 TECHNICAL REQUIREMENTS

This document should constitute the Offeror's to the items described in Section 8 of the RFP, and must contain at least the following information:

6.1 Cloud Solutions Narrative

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

6.1.1 Understanding & Overview

VIP's proposed SaaS offering, Meridian LMS, supports learning and knowledge (enterprise training and learning management) initiatives in many of the world's leading organizations and government agencies. VIP and Meridian understand the importance of having the right systems in place to attain a high-performing enterprise and how these solutions can directly lead to higher levels of productivity. Our Meridian LMS delivers and manages mission-critical training compliance initiatives with our cloud SaaS offerings.

Meridian uses best of breed technologies from Cisco, F5, Dell, NetApp, and VMware to help us deliver a robust SaaS cloud that support organizations of all sizes and in all industries. Meridian LMS is provided with a 99.7% availability guarantee. Meridian provides Disaster Recovery, Incident Response, and Business Continuity plans which are tested annually to ensure compliance. VIP has extensive experience working side-by-side with clients to deploy their learning platforms leveraging Meridian LMS. We also have extensive experience operating within highly secure organizations and helping them prepare applications as additions to approved product lists. This includes organizations within the intelligence community, such as the US Department of Defense (DoD), the US Department of Homeland Security (DHS), as well as major pharmaceutical clients. The sections below provide additional detail on VIP's ability and approach to supporting the NASPO ValuePoint Cloud Solutions Master Agreement.

6.1.2 Ability & Approach

VIP and Meridian's experienced operations team manages the entire technology stack to ensure an optimal experience is delivered to our customers.

VIP's proposed SaaS solution, Meridian LMS, offerings include the following:

- 100% Meridian Managed Environment
- State-of-the-art Facilitates & Security
- Redundant, Fault-Tolerant Power & HVAC
- Redundant Network Components and Internet Service Providers (ISPs)
- Enterprise Firewall, Intrusion Detection and Intrusion Prevention
- Real-Time Network, Security, and Availability Monitoring
- Highly Available Storage Systems
- Secure Data Backups Storage & Retention

Millions of users across the globe depend on Meridian solutions. Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in

Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II compliant. Because of the area's strategic importance as the Eastern hub of traffic exchange to the United States, Equinix's Ashburn data center campus represent one of the largest Internet exchange points in the world. Equinix provides peering and traffic exchange services for large networks, carriers and ISPs from all over the globe.

Our operational cloud environment is located in dedicated, secure co-located, space and takes advantage of some of the industry's most advanced security, power, cooling, and emergency management technologies to provide an industry-leading 99.9999% facility uptime record. Within this environment we offer reliable infrastructure, fast connectivity, and 24x7 system/network monitoring. This state-of-the-art data center is built to ensure efficient, reliable and continuous operations - even in the event of severe natural or man-made catastrophes.

Physical Security

The physical security of the data center is one of our highest priorities. Physical access is tightly controlled and restricted to preauthorized personnel only. Preauthorized access is approved only for those that have an ongoing need to support Meridian hardware.

The data center utilizes an array of security equipment, techniques and procedures to control, monitor and record access to the facilities including:

- Manned by onsite security on a 24x7x365 basis
- All doors, including cages, are secured with biometric hand geometry readers
- CCTV digital camera coverage of entire center, including cages, with archival system
- A silent alarm and automatic notification of appropriate law enforcement officials protect all exterior entrances
- CCTV integrated with access control and alarm system
- Motion-detection for lighting and CCTV coverage
- All equipment checked/screened upon arrival
- Visitors are screened upon entry to verify their identity, and in shared situations, are escorted to their appropriate locations
- Shipping and receiving area walled off from co-location areas Firewalls and Intrusion Prevention

Threat Prevention

Meridian utilizes fully redundant firewalls, intrusion detection, and intrusion prevention devices from Cisco to help us protect our customer's systems from external threats and help meet ever-increasing compliance mandates. Cisco is one of the most trusted and widely-deployed providers of firewall and threat prevention technology in the world. They invest hundreds of millions of dollars in security research, employs hundreds of threat analysts, and ingest terabytes of threat data into their threat database every day. Our intrusion prevention system is integrated into redundant firewalls, switch, and router platforms, is constantly updated from Cisco's threat database, and collaborates with other key network components for maximum protection and flexibility.

Our threat prevention accurately identifies, classifies, and stops malicious traffic before it can affect underlying systems. We defend against zero-day attacks using Anomaly Detection and 6,500 stateful, vulnerability-based signatures that protect against tens of thousands of current and future exploits. We also inspect a wide variety of protocols to ensure Request for Comment (RFC) conformance and prevent hacks.

Anti-Virus

Meridian utilizes industry leading Anti-Virus solutions from McAfee to protect against system viruses, spyware, and malware. We employ centrally managed, policy-based controls to ensure all servers are protected. Policies ensure servers utilize real-time virus scanning, perform a weekly full scan, have the latest virus scan patches, and receive the latest definitions.

Encryption

To ensure the privacy and security of your data, Meridian uses HTTPS for all communication and encrypts all inbound and outbound traffic using 128-bit and 256-bit TLS.

When data is transmitted to Meridian LMS, it first passes through the User Interface (UI) tier. Meridian LMS does not use any plug-ins that could potentially compromise security. Actions taken through the UI tier request data from, and submit data to, a dedicated Business Logic (BL) tier.

The BL tier acts as an interface between the UI tier and the database tier and maintains data integrity. It is not directly accessible via the internet and interfaces directly with the UI tier. The BL tier connects to a customer's database via a Windows service account for that specific client that only has access to that customer's data. The database tier, is located securely on a sub-network behind our firewalls and only accessible through secured connections.

Operational data stored at rest in the database, like passwords, are secured using FIPS compliant cryptography which utilizes a one-way, irreversible hashing algorithm. Personally Identifiable Information (PII) data is not required or requested by Meridian LMS, however customers can leverage custom fields to add any data they choose. Adding PII to any system should be carefully thought out and done so with care.

Patching

It is necessary to plan for security updates and revision updates to not only our LMS software but also to any of the components supporting it. All software and hardware vendors periodically release new revisions of their product so that new security holes are resolved and new features are added. The Meridian team maintains a rigorous patching process for applying and validating patches to supporting hardware, operating systems, and supporting backend applications.

Patching and system maintenance activities occur monthly and include:

- Operating System Updates – Security updates and enhancements from the OS vendors
- Firmware Updates – Firmware updates for networking and other shared hardware devices
- Backend Software Updates – Software updates for applications supporting of Meridian LMS (SQL Server, Mail Relay, SFTP, etc.)
- Meridian LMS Updates – Software code updates to Meridian LMS

Backup & Recovery

Meridian's backup process blends multiple types of backup software and hardware to ensure the reliability of our backups. These systems build redundancy to our backup plan and ensure that a recent backup is always available, in the event it's ever needed for recovery.

Meridian's backup process includes:

- Nightly Reverse Incremental Backups of all Production Virtual Machines
- Nightly Full Database Backups and 15 Minute Log Shipping
- Nightly Offsite Encrypted and Secure Transfers to a private Amazon Web Services Virtual Tape Library

As part of our backup procedures, Meridian executes a daily verification checklist. Meridian utilizes automated systems and notifications to assist in the verification of backups; however, a member of our operations team also does a manual verification each day to ensure backups are valid.

Meridian leverages the services of AWS for secure offsite backup storage. Backup data is encrypted and securely transferred from Meridian's to the US East Region and multiple availability zones on a nightly basis. Backups are stored using both S3 and Glacier Amazon services as part of the Virtual Tape Library offering.

Customer backup data is also kept for thirty (30) days onsite for quick access in the rare event that it is needed for immediate recovery.

6.1.3 Resources

Client-side resources for our cloud solution are minimal by design. All that is required to use Meridian LMS is a supported web browser and internet connectivity. Meridian resources required to run the cloud solution include: personnel, technology, infrastructure, and security testing resources.

Personnel Resources

Meridian's IT team and hosting security team are staffed by network engineers, security experts, and other personnel who monitor the SaaS environment, provide upgrades, provide maintenance, and otherwise ensure that the 99.7% availability guarantee is met. **Section 6.2.3.1** contains a list of personnel used to deploy our cloud solution.

VIP also provides value added professional services for deployment of the cloud Meridian LMS including implementation, integration, migration, support, training, and other managed services. Additional resources such as project managers, developers, business analysts, graphic designers, support staff, and database administrators are provided to fulfil value-added and/or managed services per the requirements of the specific project's timeline.

Technology Resources

The SaaS environment is monitored in real time by Meridian's monitoring and logging solution. The technologies we use to deliver our SaaS Cloud have been described in detail throughout this response and include:

- Monitoring Tools

- Logging Tools
- Reporting Tools
- Anti-Virus (McAfee)
- Threat Detection and Prevention (CISCO IPS)
- Encryption Methods (128-bit and 256-bit TLS)
- Patching tools for OS, Firmware, Backend Software, and Meridian LMS upgrades

Infrastructure Resources

Millions of users across the globe depend on Meridian solutions. Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II compliant. Because of the area's strategic importance as the Eastern hub of traffic exchange to the United States, Equinix's Ashburn data center campus represents one of the largest Internet exchange points in the world. Equinix provides peering and traffic exchange services for large networks, carriers and ISPs from all over the globe.

Meridian leverages the services of AWS for secure offsite backup storage. Backup data is encrypted and securely transferred from Meridian's to the US East Region and multiple availability zones on a nightly basis. Backups are stored using both S3 and Glacier Amazon services as part of the Virtual Tape Library offering.

Security Testing Resources

Meridian utilizes a third-party security services firm to perform an annual assessment of our information security measures and identify any security vulnerabilities. The assessment includes an external penetration (Pen) test performed by a team comprised of experienced and credentialed security engineers holding industry recognized certifications from leading institutions such as ISC2, PCI SSC, and SANS.

The Pen test is compliant with NIST Special Publication 800-115 and leverages over 60,000 tests to discover key systems, network, processes and identify application vulnerabilities in publicly accessible computer systems and network devices.

6.1.4 Options or Alternatives Proposed

Meridian offers two options for cloud deployments that are being proposed:

1) Multi-Tenant (SaaS Cloud)

2) Single-Tenant (Private SaaS Cloud)

Both options receive the same hosting services, multi-tenant (SaaS Cloud) clients are on shared hardware while single-tenant (Private SaaS Cloud) clients are on dedicated hardware. Multi-tenant (SaaS Cloud) clients receive product upgrades at once and are all on the same version, while single-tenant (Private SaaS Cloud) clients have some flexibility on when they deploy upgrades and which product versions they deploy.

6.2 Response to Technical Requirements

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

If applicable to an Offeror's Solution, an Offeror must provide a point by point response to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

6.2.1 Technical Requirements

8.1.1 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

Millions of users across the globe depend on Meridian solutions. Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II compliant. Meridian's SaaS Learning Management System (platform) and network architecture meet the following areas of NIST:

- **On demand self-service**-web hosted application
- **Resource pooling**-multiple app servers in HLA environment (clustering)
- **Monitoring and NOC monitors**—alerts of incidents via monitoring tools (Solarwinds and Site24x7)
- **Rapid Elasticity**—add and remove resources to increase computing power
- **Measured service**—monitor test pages of all clients, and provide server level monitoring

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of **Attachments C & D**.

VIP has reviewed and will comply with the requirements of Attachments C & D.

8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in **Attachment D**.

VIP acknowledges this requirement and has responded accordingly.

6.2.2 (E) Subcontractors (8.2)

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

VIP does not intend to use subcontractors to provide cloud solutions or value-added services. Our proposed SaaS offering manufacturer, Meridian, does not use subcontractors to deliver hosting services. All IT and hosting personnel are in-house employees and we have provided hosting services in-house for 20+ years. These subcontracting requirements are not applicable to Meridian.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

VIP does not intend to use subcontractors to provide cloud solutions or value-added services. Our proposed SaaS offering manufacturer, Meridian does not use subcontractors to deliver hosting services. All IT and hosting personnel are in-house employees and we have provided hosting services in-house for 20+ years. These subcontracting requirements are not applicable to Meridian.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

VIP does not intend to use subcontractors to provide cloud solutions or value-added services. Our proposed SaaS offering manufacturer, Meridian does not use subcontractors to deliver hosting services. All IT and hosting personnel are in-house employees and we have provided hosting services in-house for 20+ years. These subcontracting requirements are not applicable to Meridian.

6.2.3 (E) Working with Purchasing Entities (8.3)

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

Personnel

Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved:

- Jonna Ward, Chief Executive Officer, provides Executive Sponsorship from VIP.
- Steve Carpenter, Vice President, Administration, provides Contract and Legal support.
- Eric Scully, Contract Manager, provides communication and coordination as required between the purchasing entity, VIP, and Meridian staff.
- Geoff Perry, Chief Product Officer, provides Executive Sponsorship from Meridian.
- Wes Bowen, Director Software Architecture and Development. Mr. Bowen oversees the Hosting team and has the responsibility and authority to maintain and establish the information technology framework and operations of the organization under the direction and guidance of the leadership team. Overseas budget allocation for technical services and facilities and will coordinate the disaster recovery effort of all team members carrying a technical function.
- Ashok Cates serves as the lead Sr. Systems Engineer in the event of a disaster, with a focus on Windows Server Restoration, Security Certificates.

- Thomas Holincheck serves as lead Sr. Network Engineer for all network related design, configuration and implementation, including, firewalls, routers, switches and ISP communication and coordination. Responsibilities include data protection and security.
- Eyner Ramirez and his team serve as System Administrators and will focus on the restoration and information documentation associated with Meridian data. They will coordinate all delivery from our offsite tape facility and work with the rest of the Systems Team to rebuild and reconfigure critical core servers (both physical and virtual).
- Devin Quince and Phillip Guerrero serve as SQL Database and Build Deployment Engineer and are responsible for the backend database servers, with a focus on SQL server and central storage connectivity and configuration.

Response times

Meridian defines an "information security incident" as an event – or alleged event – directed at a Client or Client(s) hosted site (herein "Site"), computers, networks, firewalls, data centers, software, data, users and services, in violation of security policies, and circumvention of security controls that could result in gaining unauthorized access, data loss, or denial/disruption of service whether the threat source is external or internal.

Examples of incidents:

- Unauthorized access or attempts to gain unauthorized access;
- Defacing of web sites;
- Installation of Malware or virus infection;
- Denial of Service attacks whether by a known or unknown perpetuator;
- Inadvertent or deliberate destruction of data;
- Unauthorized access to or theft of restricted data; and
- Malicious activities of "insider's" with access privileges.

Meridian's logging and monitoring tools monitor client environments in real-time and key IT personnel are notified of outages and data breaches immediately. Once a Meridian IR responder has discovered suspicious or malicious activity involving the Client(s) site, or is notified via other sources, an incident ticket is created:

- Within one (1) minute for Severity 1 – Critical incidents
- Within thirty (30) minutes for Severity 2 – High incidents
- Within three (3) hours for Severity 3 – Medium incidents
- Within twenty-four (24) hours for Severity 4 – Low incidents

Incident Definitions

1. Critical Site is down or there is substantial inoperability to the Client(s) production system(s).
2. High Substantial degradation to the Client(s) primary production systems.

3. Medium Site is usable but an essential function is not performing to specifications. The condition impacts reasonable usage of the site. Loss of non-production systems.
4. Low Site is usable but not performing to specifications. The condition has minimal or no impact on the Client(s) ability to function.

Meridian has maintained a 99.7% availability rate (or greater) since we established our hosting SLAs. RTO is currently 96 hours and RPO is 24 hours.

Processes and timelines

Meridian provides defined incident response, disaster recovery, and incident response plans which govern or response times, actions, communications, reporting structure, and other critical elements in the event of a disaster. These plans are reviewed annually, tested, and employees are trained regularly on security and recovery plans. In the event of a disaster, the company will resume operations as soon as possible, preferably within 24hrs. The Emergency Response Coordinator will communicate with the chain of command as to the progress and status of operations. Program and Project Managers will communicate with clients and let them know how to contact the company as well as provide updates on operational status.

Meridian has adapted the incident handling guidelines from NIST SP800-61. Incident handling follows the four-step process:

1. Preparation
2. Detection and Analysis
3. Communication
4. Remediation (Containment, Eradication and Recovery)

Preparation

Preparation establishes the incident response capability to include personnel, implementing tools, and processes that enable Meridian to rapidly respond and effectively handle security incidents. Preparation also helps prevent incidents from occurring by ensuring that systems, networks, and applications are appropriately secured.

Preparation includes maintaining an up to date contact list, developing and maintaining procedures, identifying roles and responsibilities, and providing training for Meridian IR responders and points of contact for Client(s).

When a CAT1-3 incident occurs that has impact on a Client(s) instance, the Client(s) is notified. Notification to the Client will be as soon as possible but no later than within one (1) hour of suspected/validation/confirmation of an incident. Incidents involving Personally Identifiable Information (herein “PII”) or Personal Health Information (herein “PHI”) will be reported to the affected Client(s) within fifteen (15) minutes of detection. Details on notification are covered in Section 2.5 Email Notification below.

Detection and Analysis

Meridian has active controls and technologies in place to provide the ability to detect malicious activity through several means with varying levels of detail and fidelity. Detection and analysis, including monitoring and audit tools, are provided by the external third-party monitors that check and alert Client(s) instances monitoring for uptime and latency. Internal Meridian monitors detect service, process and system performance. Central anti-virus (herein “AV”) and Malware policies

protect and alert on malicious execution of files as well as configuration changes, and redundant Cisco® (IDS/IPS) modules (in-line with Meridian ASA Cisco® Firewalls) log, alert and blacklist the Internet Protocol (herein "IP") range of any suspicious activity deemed critical or high. All monitors are configured to alert a member of the Information Technology Operations Teams via various communication channels. The aforementioned processes and configurations allow Meridian to quickly detect and respond to suspicious or malicious activity as it is discovered.

Based on type of log event, activity or network traffic "seen," a Meridian IR responder can often make a determination if the event is a precursor to an incident that may take place in the future or an indicator that an incident is already taking place. Examples of precursors are:

- Intrusion Detection System (herein "IDS") alerts that show a port scanner or spidering tool was used against a web server
- An announcement of a new exploit that targets vulnerability in the organization's mail server
- A threat from a group stating that the group will attack the organization

Precursors are not actual incidents, but they can be clues that an attack attempt may be imminent. Indicators, on the other hand, are easier to detect because the malicious activity is occurring and events are being generated that can be observed by the Meridian IR responder using IPS/IDS alerting and logging. All traffic deemed malicious is first blocked, logged and automatically blacklisted. These alerts are stored in a central logging server for up to thirty (30) calendar days. Similarly, systems and databases are monitored real time using security auditing, SNMP traps, service/uptime detection, centralized AV policies, network usage and activity monitoring. Some examples of these are listed below:

- Insider account access privileges are subject to frequent automated account "lock outs"
- Meridian SOP's (herein "standard operating procedures") are not being adhered to
- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server
- Antivirus software alerts when it detects that a host is infected with malware
- A Meridian system administrator sees a filename with unusual characters
- A host records an auditing configuration change in its log
- A firewall control point detects unusual / suspicious activity
- An application logs multiple failed login attempts from an unfamiliar remote system
- An email administrator sees a large number of bounced emails with suspicious content
- A Meridian network administrator notices an unusual deviation from typical network traffic flows

Once a Meridian IR responder has discovered suspicious or malicious activity involving the Client(s) site, or is notified via other sources, an incident ticket is created:

- within one (1) minute for Severity 1 – Critical incidents
- within thirty (30) minutes for Severity 2 – High incidents

- within three (3) hours for Severity 3 – Medium incidents
- within twenty-four (24) hours for Severity 4 – Low incidents

The incident ticket provides a platform for automating and managing IT Service Management processes. Once inputted into Atlassian JIRA, the incident ticket can be linked to change configuration requests to remediate the issue.

Based on the activity discovered, the Meridian IR responder will flag the activity for attention by notifying management and/or conduct an investigation to determine if the activity is a precursor or indicator. This is done by looking at source and destination IP addresses and attempting to answer some basic questions that include:

- What event is taking place or triggering an alert?
- Are the IP addresses in question related to any known malicious site or group?
- What is the category of the incident (e.g. Denial of service, malicious code, unauthorized access, inappropriate usage)?
- What information is being seen in the deep packet analysis of the traffic?
- Are there attempts at ex-filtrating data? Calling home?
- Has the integrity of the Client(s) site information or data been compromised?
- Is there damage to equipment/servers?
- Could the event be the result of a failure of some security control?
- Is there evidence that several security events are related?
- Have related events been occurring over a period of time, from various locations?
- Is there evidence that more than one (1) system was involved or affected by the security event(s)?
- Could further investigation prevent future security events of this kind?

As part of the investigation, the Meridian IR responder will attempt to determine the impact of the incident on the Client(s) site and then set the Priority in the incident ticket. Priority assignment and escalation for all incidents are based on the impact and severity level of the incident, i.e. the extent of degradation of service and number of systems affected. Notification timeframe is measured from the time the incident was initially reported by the individual encountering the incident.

Communication and Assistance

Meridian's incident response plans include backup plans for Physical Communications, back up plans for Equipment and Resources, and communication escalation paths. The Employee Handbook Policy (Emergency Communications) provides a standard communication procedure to use during any emergency to communicate among employees. All employees are to be prepared and establish a plan for emergencies such as terrorism, natural disasters, severe weather, etc. A critical element of any emergency plan is communication. From the business perspective information flow is important during an emergency to let employees know what business operations are being conducted. Level and scale of the issue will dictate who communicates what

information and when. Major breaches take highest priority and receive near immediate executive communication.

Email Notification

Once the Meridian Analyst has made a determination that the suspicious activity or security event under investigation is a security incident, the initial investigative ticket created is modified to escalate to the proper priority level as described above. Within each ticket and email notification the following fields may be filled out:

- Date/time of the event
- Device Alarm Description
- Incident Summary
- Synopsis of activity/alert(s) in question
- Any prior history from researching prior Atlassian JIRA tickets
- Any prior event history
- Analysis results and recommendation from the Meridian IR responder

When the ticket has been completed and escalated to the proper category:

- The Meridian IR responder drafts a Client(s) notification email and sends to the Meridian President
- Meridian President notifies Client(s) via email and/or phone with copy to the Meridian CIRT
- For Critical CAT 1 incidents, the Meridian President will contact Client(s) directly in addition to the Meridian CIRT to expedite the notification process

Contact information for the Meridian CIRT can be found in Attachment C. The incident response form will be filled out as follows:

- The Meridian IR responder will fill out as much of the required information as they know, including whether PII and/or PHI was involved. When the file contains sensitive information, such as an IP address or an account and password, this file is password protected.
- The form will then be reviewed by the Meridian Director of Information Technology and Hosting Operations and attached to the Client(s) notification email.

All correspondence related to the incident ticket will be documented and tracked within the Atlassian JIRA ticketing system.

Remediation (Containment, Eradication, and Recovery)

Containment

For Meridian, the Meridian Director of Information Technology and Hosting Operations plays an essential part of the containment process because Meridian applies best practices to systems, maintains secure configurations, has redundant physical IPS/IDS modules and firewalls that are always up to date with the latest operating systems and patches. Further Meridian maintains logs, uses real-time alert systems, and enforces firewall rules that limit traffic to only trusted ports,

communication protocols, and limit access. These protocols and policies are the first line of defense against attacks at the infrastructure level and are the responsibility of the Meridian Director of Information Technology and Hosting Operations. One of the most important factors to the Meridian IR Plan is how fast the incident is detected and contained within the environment. It is vital to make sure that when malicious activity or policy violations are detected that the proper steps are taken to stop the threat and minimize damage to Meridian and Client(s) assets as quickly as possible.

Once a Meridian Analyst has completed the initial investigation of observed security events and declares an incident is taking place, containment becomes a priority.

Based on Severity and Potential Impact to the Client(s) site and the resident data, the Meridian Director of Information Technology and Hosting Operations is granted authority by the Client(s) Site Owner to immediately isolate the application (as necessary) to prevent potential data loss or collateral impacts from malicious activity or cyber-attacks.

Following are some examples of potential incident responses:

Cyber Attacks - Denial-Of-Service Attacks:

- Identify the source IP address of the attack on the external firewall and implement the access control rule to block that source IP address at the firewall and external router.
- Configure the external IDS to perform “TCP Reset” and “Firewall Reconfiguration” over the source IP address of the attack.

Malicious Code - Virus/Worm:

- Disconnect the system from the network which is infected with the virus.
- Update the anti-virus signature on the system and scan the computer at both the operating system level and boot level (if possible).
- Verify the vendor site for any tool which will scan the system for the presence of viruses or worms on the system.
- Alert all users of the existence of the virus/worm and the manner in which it replicates, including instructions to follow in the event their workstations are infected.

Loss or theft of data (including PII and/or PHI):

- Identify and document the recipient of the data (if possible).
- Investigate method of loss of data (electronic, media).

Unauthorized Access Attempts:

- Disable access attempt method by disabling account.
- Investigate access attempts through audit logs.

Malicious Activity – Insider:

- Disable account access
- Investigate activity conducted using account access through logs.
- Repair/restore system.

The notice from the Meridian Director of Information Technology and Hosting Operations to Client(s) will go out at the same time as the containment process is taking place.

When malicious source IP addresses are discovered they are immediately blocked by the physical IPS module within Meridian's redundant ASA firewalls. This will prevent and contain any further attacks from impacting Client(s). These steps are also included in the incident ticket and Client(s) notification for accountability and tracking.

During this time, evidence is gathered by the Meridian Director of Information Technology and Hosting Operations. This information will be accounted for within the Atlassian JIRA incident ticket along with any correspondence related to the incident. The Meridian Director of Information Technology will notify the Client(s) of activity as it is taking place throughout the incident response period to enable reporting to outside Government Agencies having jurisdiction over such incidents if required.

Eradication and Recovery

Systems and service capabilities may remain "offline" until eradication and certification is completed and Client(s) grants formal approval to re-use.

Once all the proper steps have been taken and all the evidence has been gathered the Meridian Director of Information Technology and Hosting Operations will make the recommendations to remove any malicious code or program. Actions taken during the recovery phase may include, but is not limited to:

- Responder Team restoring systems to normal operations
- Remediate vulnerabilities to prevent similar incidents from recurring
- Restoring site from clean backups
- Rebuilding site from scratch
- Replacing compromised files with clean versions
- Installing patches or updates
- Changing passwords
- Tightening network perimeter security (e.g., firewall rule sets, boundary router access control lists)

From information that is discovered during the investigation the Meridian Director of Information Technology and Hosting Operations can create custom IPS rules based on the traffic and file/s that caused the incident to take place. The rules can then be set to block all traffic which will reduce the likelihood of future attacks.

Reporting Incidents

If a Client(s) notices any suspicious or questionable activities that result in a security incident, the Client(s) should report incidents to the Meridian Director of Information Technology and Hosting Operations. If that person is unavailable, the Client(s) may contact anyone listed in Attachment C.

Meridian Director of Information Technology and Hosting Operations can be reached via phone at (703) 261-7272.

When contacting the Meridian Director of Information Technology and Hosting Operations, Client(s) should include as much information as possible. This information should cover, but is not limited to the following:

- Exhibited Site Impact / Effect (Users can't log in, systems performance degradation; missing or improperly formatted pages and or functionality)
- Source and Destination IP
- Date and time that event was noticed
- Source and Destination Port
- Summary of the issue
- As much descriptive detail as possible that is known at the time
- Points of contact information

Upon reporting, the Meridian Director of Information Technology and Hosting Operations will send an email notification of receipt and include an incident ticket number for reference and tracking. Details of reporting incidents to the Meridian Director of Information Technology and Hosting Operations include:

- Notification must take place within one (1) hour of suspecting/confirming an incident has occurred or as reasonably practical.
- Notification must take place within fifteen (15) minutes of suspecting/confirming an incident involving PII and/or PHI has occurred or a reasonably practical.
- The Meridian Director of Information Technology and Hosting Operations will apprise Client(s) of response activities performed/completed throughout duration of the incident or until incident report closure.

Other information vital to understanding the service you provide

Meridian provides a monitoring and logging system that will notify our IT personnel of outages, data breaches, and other potential malicious actions in real-time. Meridian provides defined incident response, disaster recovery, and incident response plans which govern response times, actions, communications, reporting structure, and other critical elements in the event of a disaster, breach, or outage.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Meridian employees undergo regular business ethics and anti-trust training (at least annually) and employees who push adware, software, or marketing not authorized by the participating entity or master agreement face disciplinary action to include termination.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Meridian clients receive a stage environment identical to production for testing changes to the system prior to moving them to production environment.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

Meridian is focused on building software that is accessible by as many users as possible. Meridian follows the implementation techniques and guidelines of the World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG). Meridian Global complies with the accessibility standards as per Section 508 of the Rehabilitation Act, which requires all US government organizations to make their Web content accessible to the disabled.

Meridian has a long history of working with customers in the public sector (both Federal and State government), many of which require compliance with Section 508 standards. We have worked closely with the Office of Accessible Systems and Technology (OAST) specifically in support of the agencies supporting the Department of Homeland Security (DHS). As such we employ OAST-certified testers to help us validate compliance with accessibility standards as part of our standard software development and testing lifecycle.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

All that is required to use Meridian LMS is a supported web browser and internet connectivity. We recommend the latest versions of commonly used browsers such as Chrome, FireFox, Safari, and Internet Explorer.

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

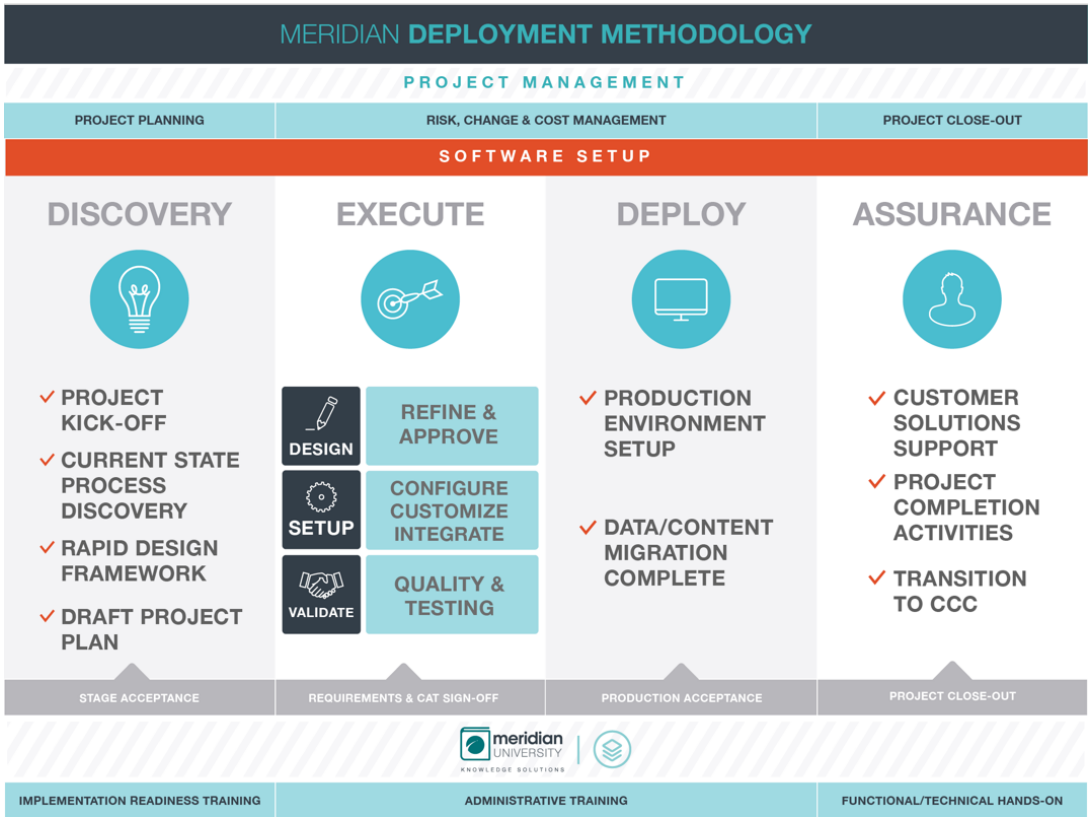
Meridian solution consultants, technical personnel, and legal advisors will engage potential purchasing entities with pre-sales consulting prior to execution of the SLA to take personally identifiable information into consideration. This includes recommendations and plans for storing sensitive data and compliance consulting for local and federal regulations (where applicable). Our Learning Management System does not store sensitive personal information (such as social security numbers or credit card numbers) by default, most data elements in our system are training related (such as course completions, grades, test scores, etc.). Any data communicated between integrated systems is encrypted to ensure safety during transit.

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

We have provided implementation details, project management plan details, and a sample project timeline below for Meridian LMS.

Implementation

Figure 1: Meridian's implementation methodology is based upon 20+ years' experience delivering our own solutions with in-house employees.



Implementation Plan:

Meridian's implementation methodology is based upon 20+ years of proven experience and meets industry standards (PMBOK, etc.). Change control, communications, risk, and other ancillary services are also supported and our PMO provides project management planning and delivery oversight for the duration of the implementation. Further, all Meridian project managers are PMP certified.

Meridian's standard implementation is 8-12 weeks. A sample 12-week timeline is included below.

- Week 1: Project kickoff
- Weeks 2-5: Discovery Phase: Project planning, client business and functional requirements gathering, and requirements sign-off
- Weeks 6-10: Execution Phase: Design, Configurations, Development, Integrations, Customer Acceptance Testing, and sign-off
- Weeks 11-12: Production environment setup, customer go-live, and project acceptance

Sample Project Timeline

A sample project timeline indicative of a standard 12-week implementation begins on the following pages.

Figure 2: Sample Project Timeline

ID	WBS	Task Name	% Complete	Duration	Start	Finish
1	**1**	**Meridian Global Implementation**	**0%**	**77 days**	**Mon 1/1/18**	**Tue 4/17/18**
2	**1.1**	**Project Initiation**	**0%**	**10.25 days**	**Mon 1/1/18**	**Mon 1/15/18**
3	1.1.1	Internal Sales Handoff Meeting	0%	1 day	Mon 1/1/18	Mon 1/1/18
4	**1.1.2**	**Project Kickoff**	**0%**	**5 days**	**Tue 1/2/18**	**Mon 1/8/18**
5	1.1.2.2	Set up Project in JIRA Ticketing & Financial Systems	0%	1 day	Tue 1/2/18	Tue 1/2/18
6	1.1.2.3	PM to PM Meeting	0%	1 day	Wed 1/3/18	Wed 1/3/18
7	1.1.2.4	Conduct Project Kickoff Meeting with Client	0%	1 day	Mon 1/8/18	Mon 1/8/18
8	**1.1.3**	**Set up Local Environments & Base Installation**	**0%**	**7.25 days**	**Thu 1/4/18**	**Mon 1/15/18**
9	1.1.3.1	Set up Meridian Environments (Dev, QA, Stage)	0%	5 days	Thu 1/4/18	Wed 1/10/18
10	1.1.3.2	Setup SFTP Site	0%	1 day	Thu 1/4/18	Thu 1/4/18
11	1.1.3.3	Validate Meridian Local Environments and SFTP Site	0%	1 day	Thu 1/11/18	Thu 1/11/18
12	1.1.3.4	Load Baseline Documentation into SFTP	0%	1 day	Thu 1/11/18	Thu 1/11/18
13	1.1.3.5	Create Accounts for Client in Stage	0%	0.5 days	Thu 1/11/18	Thu 1/11/18
14	1.1.3.6	Send Stage URL to Client PM	0%	0.25 days	Fri 1/12/18	Fri 1/12/18
15	1.1.3.7	MILESTONE - Obtain Sign-off of Staging Environment Access	0%	0 days	Mon 1/15/18	Mon 1/15/18
16	**1.2**	**Project Planning**	**0%**	**6 days**	**Tue 1/9/18**	**Tue 1/16/18**
17	**1.2.1**	**Develop Project Schedule**	**0%**	**6 days**	**Tue 1/9/18**	**Tue 1/16/18**
18	1.2.1.1	Draft Project Schedule	0%	2 days	Tue 1/9/18	Wed 1/10/18
19	1.2.1.2	Send Draft Project Schedule to client	0%	1 day	Thu 1/11/18	Thu 1/11/18
20	1.2.1.3	Review Schedule and send task additions, if applicable	0%	2 days	Fri 1/12/18	Mon 1/15/18
21	1.2.1.4	Integrate client tasks into schedule and baseline	0%	1 day	Tue 1/16/18	Tue 1/16/18
22	**1.3**	**Analysis/Discovery**	**0%**	**12.5 days**	**Wed 1/17/18**	**Fri 2/2/18**
23	**1.3.2**	**Conduct Requirements Planning & Analysis**	**0%**	**0.5 days**	**Wed 1/17/18**	**Wed 1/17/18**
24	1.3.2.1	Conduct Configuration Workbook Session	0%	0.5 days	Wed 1/17/18	Wed 1/17/18
25	1.3.2.5	Conduct Joint Requirements Review Session	0%	0.5 days	Wed 1/17/18	Wed 1/17/18
26	1.3.2.6	MILESTONE - Obtain client Sign-off of Configurations Workbook	0%	0 days	Wed 1/17/18	Wed 1/17/18
27	**1.3.3**	**Requirements**	**0%**	**9 days**	**Wed 1/17/18**	**Tue 1/30/18**
28	**1.3.3.1**	**Development & Review of Functional Requirements**	**0%**	**9 days**	**Wed 1/17/18**	**Tue 1/30/18**
29	1.3.3.1.1	Develop Data Migration functional requirements	0%	3 days	Wed 1/17/18	Mon 1/22/18
30	1.3.3.1.4	Send functional requirements to Client	0%	1 day	Mon 1/22/18	Tue 1/23/18
31	1.3.3.1.5	Review and approve functional requirements	0%	5 days	Tue 1/23/18	Tue 1/30/18
32	1.3.3.1.6	MILESTONE - Functional Requirements Complete	0%	0 days	Tue 1/30/18	Tue 1/30/18
33	**1.3.4**	**Design**	**0%**	**3 days**	**Tue 1/30/18**	**Fri 2/2/18**
34	**1.3.4.1**	**Develop Technical Approach & Design Document**	**0%**	**3 days**	**Tue 1/30/18**	**Fri 2/2/18**

ID	WBS	Task Name	% Complete	Duration	Start	Finish
35	1.3.4.1.1	Develop Technical Approach for Data Migration	0%	3 days	Tue 1/30/18	Fri 2/2/18
36	1.3.4.1.4	MILESTONE - Internal Design Complete	0%	0 days	Fri 2/2/18	Fri 2/2/18
37	**1.4**	**Configuration & Theming Implementation**	**0%**	**19 days**	**Wed 1/17/18**	**Tue 2/13/18**
38	**1.4.1**	**Implement Configurations**	**0%**	**7 days**	**Fri 2/2/18**	**Tue 2/13/18**
39	1.4.1.1	Implement Configuration Settings from Configurations Workbook to QA site	0%	1 day	Fri 2/2/18	Mon 2/5/18
40	1.4.1.2	QA Testing of configurations settings	0%	1 day	Mon 2/5/18	Tue 2/6/18
41	1.4.1.3	Implement Configuration Settings to Stage site	0%	1 day	Tue 2/6/18	Wed 2/7/18
42	1.4.1.6	Client configuration of system settings through UI in Stage	0%	2 days	Wed 2/7/18	Fri 2/9/18
43	1.4.1.7	Client review and approve Configurations	0%	2 days	Fri 2/9/18	Tue 2/13/18
44	1.4.1.8	MILESTONE - Obtain client Sign-off of Final Configurations	0%	0 days	Tue 2/13/18	Tue 2/13/18
45	**1.4.2**	**Implement Theming**	**0%**	**8 days**	**Wed 1/17/18**	**Mon 1/29/18**
46	1.4.2.1	Complete Theming checklist and submit to Meridian	0%	2 days	Wed 1/17/18	Fri 1/19/18
47	1.4.2.2	Creation of mock-up in Stage based on checklist	0%	5 days	Fri 1/19/18	Fri 1/26/18
48	1.4.2.4	Client review and approval of mock-up	0%	1 day	Fri 1/26/18	Mon 1/29/18
49	1.4.2.10	MILESTONE - Obtain client Sign-off of Final Theming	0%	0 days	Mon 1/29/18	Mon 1/29/18
50	**1.5**	**Standard Implemenation Activities**	**0%**	**19 days**	**Tue 2/13/18**	**Mon 3/12/18**
51	**1.5.2**	**Conduct Legacy Content/Data Migration Activities**	**0%**	**17 days**	**Tue 2/13/18**	**Thu 3/8/18**
52	1.5.2.1	Send Content/Data Migration Template to client	0%	1 day	Tue 2/13/18	Wed 2/14/18
53	1.5.2.2	Create sample file for Meridian	0%	5 days	Wed 2/14/18	Wed 2/21/18
54	1.5.2.3	Receive Sample Data from Client	0%	0 days	Wed 2/21/18	Wed 2/21/18
55	1.5.2.4	Migrate Data - Iteration 1 in Dev	0%	2 days	Wed 2/21/18	Fri 2/23/18
56	1.5.2.5	Create 2nd Sample file if needed	0%	3 days	Fri 2/23/18	Wed 2/28/18
57	1.5.2.6	Migrate Data - Iteration 2 in Dev	0%	2 days	Wed 2/28/18	Fri 3/2/18
58	1.5.2.7	Execute migration in QA & Stage	0%	1 day	Fri 3/2/18	Mon 3/5/18
59	1.5.2.11	Pre Validation Testing Meridian Stage Environment	0%	3 days	Mon 3/5/18	Thu 3/8/18
60	1.5.2.12	MILESTONE - Content/Data Migration Development Complete	0%	0 days	Thu 3/8/18	Thu 3/8/18
61	**1.5.3**	**Conduct Single Sign-on Activities**	**0%**	**5 days**	**Mon 3/5/18**	**Mon 3/12/18**
62	1.5.3.1	Code/Unit Test	0%	2 days	Mon 3/5/18	Wed 3/7/18
63	1.5.3.2	Release to QA for Testing	0%	1 day	Wed 3/7/18	Thu 3/8/18
64	1.5.3.3	Meridian QA Test/Fix/Deliver	0%	1 day	Thu 3/8/18	Fri 3/9/18
65	1.5.3.4	Finalize Code/Unit Test	0%	1 day	Fri 3/9/18	Mon 3/12/18
66	1.5.3.5	MILESTONE - SSO Development Complete	0%	0 days	Mon 3/12/18	Mon 3/12/18
67	**1.11**	**Training Activities**	**0%**	**46 days**	**Fri 1/5/18**	**Fri 3/9/18**
68	**1.11.16**	**Conduct Implementation Readiness Training (IRT)**	**0%**	**8 days**	**Fri 1/5/18**	**Tue 1/16/18**

ID	WBS	Task Name	% Complete	Duration	Start	Finish
69	1.11.16.14	Finalize IRT Logistics	0%	1 day	Fri 1/5/18	Mon 1/8/18
70	1.11.16.15	Conduct IRT with Client	0%	2 days	Mon 1/15/18	Tue 1/16/18
71	**1.11.17**	**Conduct Administrative Training**	**0%**	**11 days**	**Fri 2/23/18**	**Fri 3/9/18**
72	1.11.17.18	Finalize Administrator Training Logistics	0%	1 day	Fri 2/23/18	Mon 2/26/18
73	1.11.17.19	Conduct Training with Client	0%	5 days	Mon 3/5/18	Fri 3/9/18
74	1.11.19	MILESTONE - Training Complete	0%	0 days	Fri 3/9/18	Fri 3/9/18
75	**1.7**	**Go Live Activities**	**0%**	**21 days**	**Mon 3/12/18**	**Tue 4/10/18**
76	**1.7.3**	**Client Acceptance Testing**	**0%**	**15 days**	**Mon 3/12/18**	**Mon 4/2/18**
77	1.7.3.6	Configurations	0%	5 days	Mon 3/12/18	Mon 3/19/18
78	1.7.3.7	Theming	0%	5 days	Mon 3/12/18	Mon 3/19/18
79	1.7.3.8	Data Migration	0%	5 days	Mon 3/12/18	Mon 3/19/18
80	1.7.3.9	SSO	0%	5 days	Mon 3/12/18	Mon 3/19/18
81	1.7.3.10	Dcoument UAT Issues, if applicable	0%	5 days	Mon 3/12/18	Mon 3/19/18
82	1.7.3.4	Meridian QA Test/Fix/Deliver	0%	10 days	Mon 3/19/18	Mon 4/2/18
83	1.7.3.7	MILESTONE - UAT Testing Completed	0%	0 days	Mon 4/2/18	Mon 4/2/18
84	**1.7.2**	**Go Live**	**0%**	**6 days**	**Mon 4/2/18**	**Tue 4/10/18**
85	1.7.2.1	Send Production Readiness Checklist	0%	1 day	Mon 4/2/18	Tue 4/3/18
86	1.7.2.2	Create Final Data Migration Template (blackout period begins)	0%	2 days	Mon 4/2/18	Wed 4/4/18
87	1.7.2.3	Production Install incl. Theming, Configs, and Extensions	0%	1 day	Wed 4/4/18	Thu 4/5/18
88	1.7.2.5	Production Acceptance Testing	0%	2 days	Thu 4/5/18	Mon 4/9/18
89	1.7.2.8	Final Go / No Go Decision	0%	0.5 days	Mon 4/9/18	Mon 4/9/18
90	1.7.2.6	Turn on new MG production site (blackout period ends)	0%	0.5 days	Tue 4/10/18	Tue 4/10/18
91	1.7.2.7	MILESTONE - Go Live Complete	0%	0 days	Tue 4/10/18	Tue 4/10/18
92	**1.9**	**Monitoring & Controlling Tasks**	**0%**	**60 days**	**Wed 1/17/18**	**Tue 4/10/18**
93	1.9.1	Weekly Project Status Call	0%	60 days	Wed 1/17/18	Tue 4/10/18
94	1.9.2	Weekly Updated Schedule	0%	60 days	Wed 1/17/18	Tue 4/10/18
95	1.9.3	Weekly Written Status Report	0%	60 days	Wed 1/17/18	Tue 4/10/18
96	**1.10**	**Closing**	**0%**	**5.5 days**	**Tue 4/10/18**	**Tue 4/17/18**
97	**1.10.1**	**Close Project**	**0%**	**5.5 days**	**Tue 4/10/18**	**Tue 4/17/18**
98	1.10.1.1	Send Project Acceptance Form to Client	0%	0.5 days	Tue 4/10/18	Tue 4/10/18
99	1.10.1.2	MILESTONE - Client Signs & Returns Project Acceptance Form	0%	5 days	Wed 4/11/18	Tue 4/17/18
100	1.10.1.3	Conduct CCC Transition Meeting	0%	1 day	Wed 4/11/18	Thu 4/12/18
101	1.10.1.4	MILESTONE - Transition to Customer Support Center Completed	0%	0 days	Thu 4/12/18	Thu 4/12/18

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.

  During the term of the Master Agreement(s), VIP anticipates a need to update the awarded Solutions as services are introduced or removed from VIP's offerings.

  VIP's new services that are introduced as an update will meet the minimum specifications and terms and conditions outlined in the resulting master agreement and in VIP's response to this solicitation.

  VIP's new additions with accompanying terms and conditions will not diminish or weaken existing terms and conditions in the judgment of the State of Utah (Lead State).

  Pricing will utilize the same pricing structure as was used for services falling into the same service category. The same minimum discount prices identified on VIP's cost proposal will apply to the new solutions and services.

- How Offeror will maintain discounts at the levels set forth in the contract.

  VIP will maintain the same minimum discount percentages for the duration of the contract, including with updates or the addition of new services.

- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.

  VIP will report, as needed, changes in technology and make recommendations for services updates. Meridian provides periodic updates to clients including publication of annual maintenance schedules (at the beginning of each year), new product releases, and the IT communicates any critical patches applied. Clients are included in the new release testing process and receive the opportunity to test new features before they become generally available and they have ample notice of impending upgrades (typically more than one month). Ongoing consulting is provided from a Customer Success Manager applied to each client to educate clients on impending feature changes, new trends, emerging technologies, and potential value-added services.

- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

  Our service teams are provided in-house providing direct accountability in service delivery. We work with our clients not only as a SaaS solution provider but as 22+ year consulting veterans. We provide documented and proven change control and risk management methodologies to mitigate change risks and other project risks. Additional Project support services (value added services) can be provided as additional project services to further mitigate transition and change risks.

6.2.4 (E) Customer Service (8.4)

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

Quality assurance measures;

Escalation plan for addressing problems and/or complaints; and

Service Level Agreement (SLA).

Meridian's primary method of ensuring excellent customer support is through ongoing consulting provided from a customer success manager assigned to learn each client's business drivers, build trust, manage the relationship, and serve as the primary point of escalation. Success mangers are our client's advocates within Meridian and they provide monthly health checks and other ongoing support and consulting services. Clients additionally have the option to join our client community and client advisory teams to share best practices and contribute to the direction of our product.

Clients are supported by the Customer Care Center (CCC) for ongoing issues like bugs, technical questions, and "how-to" questions. The CCC triages issues by severity and each severity level has an accompanying response time SLA and corresponding escalation path (defined in our customer support policy). For instance, critical issues that may impact our 99.7% availability guarantee have a response time of one hour, while minor issues such as a small bug may not be resolved until monthly maintenance is performed or a new version is released. The CCC is available to client administrators from 8 AM to 8 PM (EST) by phone, email, and support portal. 24x7 support and end user support options are also available.

Quality assurance is provided in 3 critical areas:

1) **Product Development:** Meridian's development and ongoing improvement philosophy leads to two application upgrades per year. Quality in development includes client testing, employee "bug bashes," and our processes follow industry standard agile development processes for quality.

2) **Software Deployment:** Meridian's standard software deployment processes include User Acceptance Testing and a master test plan to ensure the Meridian LMS is implemented to client quality specifications.

3) **Network Management:** Meridian's architecture and infrastructure are continually evaluated for quality and security risk. Network quality improvements, security features, and other hosted-service quality methods are applied as required. Meridian has defined Disaster Recovery, Incident Response, and Business Continuity plans that are tested annually. Meridian employees receive annual security training to ensure security risks are minimalized and that quality is maximized.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

Each Meridian client receives a customer success manager to serve as the lead representative for Meridian to our clients.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

Meridian support is available by phone from 8 AM to 8 PM EST to cover standard 8-5 business hours in all US time zones. Additional extended 24x7 support options are available for clients who require 24x7 phone support. The CCC is 24x7 and after-hours support requests may be submitted by email or portal.

c. Customer Service Representative will respond to inquiries within one business day.

The CCC responds to within inquiries within one business day. The CCC acknowledges receipt and provides updates according to severity. CCC triages issues by severity and each severity level has an accompanying response time SLA and corresponding escalation path (defined in our customer support policy). For instance, critical issues that may impact our 99.7% availability guarantee have a response time of one hour, while minor issues such as a small bug may not be resolved until monthly maintenance is performed or a new version is released.

d. You must provide design services for the applicable categories.

Meridian provides UI and UX design consulting services as part of our professional services offering to clients. Our product is easy to use and we put design capabilities in the hands of the clients, often negating the need for Meridian services. These types of services are provided for clients who request/require them.

e. You must provide Installation Services for the applicable categories.

Meridian provides implementation and installation services including project management, quality assurance, risk management, communications, migration, integration, hosting, and support.

6.2.5 (E) Security of Information (8.5)

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Data integrity and protection are critical aspects of Meridian’s hosting security profile. From a technology perspective, we approach data security Physically, Virtually, and within the Meridian LMS application. Meridian utilizes fully redundant firewalls, intrusion detection, and intrusion prevention devices from Cisco to help us protect our customer’s systems from external threats and help meet ever-increasing compliance mandates. Cisco is one of the most trusted and widely-deployed providers of firewall and threat prevention technology in the world. They invest hundreds of millions of dollars in security research, employs hundreds of threat analysts, and ingest terabytes of threat data into their threat database every day. Our intrusion prevention system is integrated into redundant firewalls, switch, and router platforms, is constantly updated from Cisco’s threat database, and collaborates with other key network components for maximum protection and flexibility.

Our threat prevention accurately identifies, classifies, and stops malicious traffic before it can affect underlying systems. We defend against zero-day attacks using Anomaly Detection and 6,500 stateful, vulnerability-based signatures that protect against tens of thousands of current and future

exploits. We also inspect a wide variety of protocols to ensure Request For Comment (RFC) conformance and prevent hacks.

Privacy & Data Collection

Meridian follows the minimum necessary standard in collecting and storing information needed for the operation of our software. Normal operation of Meridian LMS does not require any sensitive information such as a SSN or date of birth for users. If ecommerce features are used, payment card information such as credit card numbers, are never stored by Meridian. Information such as IP address of a user accessing the system may be collected for analytical and security purposes, but not retained more than 90 days.

Meridian is Privacy Shield certified and remains committed to support privacy standards set forth in in the Generally Accepted Privacy Principles (GAPP) and EU General Data Protection Regulation (GDPR).

Access Control

Access to customer data is tightly controlled. Normal staff do not have access to customer systems or data contained within them. A small group of key operations support staff, do have access to customer data and systems as it is required for ongoing support, operation, and backup of the Meridian LMS.

There are times when elevated access as read-only (or with write-access) may be needed by another team member to maintain, troubleshoot, or resolve issues related to customer production (or lower environment) systems. If this need arises, a detailed request including the type of access and duration needed must be submitted for approval. Elevated access requests are reviewed and only approved on a need-to-have basis. Once elevated access is granted, it will be available for the time specified and only for the customer (and environments) for which it was approved.

Security Policy

Meridian recognizes technology is only part of a total security solution. Along with technology, Meridian ensures security policy, procedures, and organizational security awareness are applied in a systematic manner. Meridian conducts annual security awareness training for all staff, as well as annual review of IT security policies with key operational staff.

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Meridian follows the minimum necessary standard in collecting and storing information needed for the operation of our software. Normal operation of Meridian LMS does not require any sensitive information such as SSN or date of birth for users. If ecommerce features are used, payment card information such as credit card numbers, are never stored by Meridian. Information such as IP address of a user accessing the system may be collected for analytical and security purposes, but not retained more than 90 days.

Meridian is Privacy Shield certified and remains committed to support privacy standards set forth in in the Generally Accepted Privacy Principles (GAPP) and EU General Data Protection Regulation (GDPR).

8.5.3 Offeror must describe how it will not access a Purchasing Entity’s user accounts or data, except in the course of data center operations, response to service or technical issues, as required

by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Access to customer data is tightly controlled. Normal staff do not have access to customer systems or data contained within them. A small group of key operations support staff do have access to customer data and systems as it is required for ongoing support, operation, and backup of the Meridian LMS.

There are times when elevated access as read-only (or with write-access) may be needed by another team member to maintain, troubleshoot, or resolve issues related to customer production (or lower environment) systems. If this need arises, a detailed request including the type of access and duration needed must be submitted for approval. Elevated access requests are reviewed and only approved on a need-to-have basis. Once elevated access is granted, it will be available for the time specified and only for the customer (and environments) for which it was approved.

6.2.6 (E) Privacy and Security (8.6)

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in **Attachment D**, including supporting the different types of data that you may receive.

Millions of users across the globe depend on Meridian solutions. Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II compliant. Meridian is committed to maintaining and exceeding industry standards for IT and SaaS hosting certifications including NIST 800-54/FISMA certification.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror’s proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Millions of users across the globe depend on Meridian solutions. Meridian hosted solutions are handled by secure, state-of-the-art data center located in Equinix's IBX Data Center campus in Ashburn, VA and are HIPAA, ISO 27001, NIST 800-53/FISMA, PCI DSS, SOC 1 Type II, SOC 2 Type II (SSAE16) compliant. Meridian’s SaaS Learning Management System (platform) and network architecture meet the following areas of NIST:

- **On demand self-service**-web hosted application
- **Resource pooling**-multiple app servers in HLA environment (clustering)
- **Monitoring and NOC monitors**—alerts of incidents via monitoring tools (Solarwinds and Site24x7)
- **Rapid Elasticity**—add and remove resources to increase computing power
- **Measured service**—monitor test pages of all clients, and provide server level monitoring

Meridian LMS does not store credit card information (PCI), medical information (HIPAA), or social security numbers.

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Meridian maintains significant real-world experience and expertise in developing secure LMS solutions for organizations of all sizes, complexity, and sophistication. We utilize some of the most advanced technology and solutions available for internet security.

Industry-Leading Data Center Facilities

Meridian's operational cloud environment is located in our dedicated, secure space co-located within Equinix's IBX data center campus in Ashburn, VA. Because of the area's strategic importance as the Eastern hub of traffic exchange to the United States, Equinix's Ashburn data center campus represents one of the largest Internet exchange points in the world. Equinix provides peering and traffic exchange services for large networks, carriers and ISPs from all over the globe.

Our cloud takes advantage of some of the industry's most advanced security, power, cooling, and emergency management technologies to provide an industry-leading 99.9999% facility uptime record. Within this environment we offer reliable infrastructure, fast connectivity, and 24x7 system/network monitoring. This state-of-the-art data center is built to ensure efficient, reliable and continuous operations - even in the event of severe natural or man-made catastrophes.

Physical Security

The physical security of the data center is one of our highest priorities. Physical access is tightly controlled and restricted to preauthorized personnel only. Preauthorized access is approved only for those that have an ongoing need to support Meridian hardware.

The data center utilizes an array of security equipment, techniques and procedures to control, monitor and record access to the facilities including:

- Manned by onsite security on a 24x7x365 basis
- All doors, including cages, are secured with biometric hand geometry readers
- CCTV digital camera coverage of entire center, including cages, with archival system
- A silent alarm and automatic notification of appropriate law enforcement officials protect all exterior entrances
- CCTV integrated with access control and alarm system
- Motion-detection for lighting and CCTV coverage
- All equipment checked/screened upon arrival
- Visitors are screened upon entry to verify their identity, and in shared situations, are escorted to their appropriate locations
- Shipping and receiving area walled off from co-location areas Firewalls and Intrusion Prevention

Threat Prevention

Meridian utilizes fully redundant firewalls, intrusion detection, and intrusion prevention devices from Cisco to help us protect our customer's systems from external threats and help meet ever-increasing compliance mandates. Cisco is one of the most trusted and widely-deployed providers of firewall and threat prevention technology in the world. They invest hundreds of millions of dollars in security research, employs hundreds of threat analysts, and ingest terabytes of threat data into their threat database every day. Our intrusion prevention system is integrated into redundant firewalls, switch, and router platforms, is constantly updated from Cisco's threat database, and collaborates with other key network components for maximum protection and flexibility.

Our threat prevention accurately identifies, classifies, and stops malicious traffic before it can affect underlying systems. We defend against zero-day attacks using Anomaly Detection and 6,500 stateful, vulnerability-based signatures that protect against tens of thousands of current and future exploits. We also inspect a wide variety of protocols to ensure Request For Comment (RFC) conformance and prevent hacks.

Anti-Virus

Meridian utilizes industry leading Anti-Virus solutions from McAfee to protect against system viruses, spyware, and malware. We employ centrally managed, policy-based controls to ensure all servers are protected. Policies ensure servers utilize use real-time virus scanning, perform a weekly full scan, have the latest virus scan patches, and receive the latest definitions.

Encryption

To ensure the privacy and security of your data, Meridian uses HTTPS for all communication and encrypts all inbound and outbound traffic using 128-bit and 256-bit TLS.

When data is transmitted to Meridian LMS, it first passes through the User Interface (UI) tier. Meridian LMS does not use any plug-ins that could potentially compromise security. Actions taken through the UI tier request data from, and submit data to, a dedicated Business Logic (BL) tier.

The BL tier acts as an interface between the UI tier and the database tier and maintains data integrity. It is not directly accessible via the internet and interfaces directly with the UI tier. The BL tier connects to a customer's database via a Windows service account for that specific client that only has access to that customer's data. The database tier, is located securely on a sub-network behind our firewalls and only accessible through secured connections.

Operational data stored at rest in the database, like passwords, are secured using FIPS compliant cryptography which utilizes a one-way, irreversible hashing algorithm. Personally Identifiable Information (PII) data is not required or requested by Meridian LMS, however customers can leverage custom fields to add any data they choose. Adding PII to any system should be carefully thought out and done so with care.

Patching

It is necessary to plan for security updates and revision updates to not only our LMS software but also to any of the components supporting it. All software and hardware vendors periodically release new revisions of their product so that new security holes are resolved and new features are added. The Meridian team maintains a rigorous patching process for applying and validating patches to supporting hardware, operating systems, and supporting backend applications.

Patching and system maintenance activities occur monthly and include:

- Operating System Updates – Security updates and enhancements from the OS vendors

- Firmware Updates – Firmware updates for networking and other shared hardware devices
- Backend Software Updates – Software updates for applications supporting of Meridian LMS (SQL Server, Mail Relay, SFTP, etc.)
- Meridian LMS Updates – Software code updates to Meridian LMS
- Backup & Recovery
- Meridian's backup process blends multiple types of backup software and hardware to ensure the reliability of our backups. These systems build redundancy to our backup plan and ensure that a recent backup is always available, in the event it's ever needed for recovery.
- Meridian's backup process includes:
  - Nightly Reverse Incremental Backups of all Production Virtual Machines
  - Nightly Full Database Backups and 15 Minute Log Shipping
  - Nightly Offsite Encrypted and Secure Transfers to a private Amazon Web Services Virtual Tape Library

As part of our backup procedures, Meridian executes a daily verification checklist. Meridian utilizes automated systems and notifications to assist in the verification of backups; however, a member of our operations team also does a manual verification each day to ensure backups are valid.

Meridian leverages the services of AWS for secure offsite backup storage. Backup data is encrypted and securely transferred from Meridian's to the US East Region and multiple availability zones on a nightly basis. Backups are stored using both S3 and Glacier Amazon services as part of the Virtual Tape Library offering.

Customer backup data is also kept for thirty (30) days onsite for quick access in the rare event that it is needed for immediate recovery.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Access to customer data is tightly controlled. Normal staff do not have access to customer systems or data contained within them. A small group of key operations support staff, do have access to customer data and systems as it is required for ongoing support, operation, and backup of the Meridian LMS.

There are times when elevated access as read-only (or with write-access) may be needed by another team member to maintain, troubleshoot, or resolve issues related to customer production (or lower environment) systems. If this need arises, a detailed request including the type of access and duration needed must be submitted for approval. Elevated access requests are reviewed and only approved on a need-to-have basis. Once elevated access is granted, it will be available for the time specified and only for the customer (and environments) for which it was approved.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Meridian is ISO 27001 compliant and our data center (Equinix IBX datacenter campus in Ashburn, VA) meets industry controls for SOC Type II compliance. Meridian LMS does not store credit card information (PCI), medical information (HIPAA), or social security numbers. Meridian is currently undergoing internal SOC I compliance audits for 2018 and anticipates being SOC II compliant in 2019. Meridian is also currently in the progress of FedRAMP compliance and sponsorship. The results of our most recent penetration test are included on the following page:

February 14, 2018

Mr. Ruben Mercado
Director IT & Hosting Operations
Meridian Knowledge Solutions
2001 Edmund Halley Drive, Suite 400
Reston, VA 20191 USA

Dear Sir:

Utilizing a team of experienced and credentialed security consultants holding industry recognized certifications from leading institutions such as ISC^2, EC-Council, PCI SSC, and SANS, nGuard recently completed an external penetration test for Meridian Knowledge Solutions. This security test focused on identifying security vulnerabilities in Meridian's environment. For this test, nGuard utilized the National Institute of Standards and Technology (NIST) standard SP 800-115 as the basis for our testing methodology. The subject area audited is detailed below along with its respective audit score. Please note that a score of 4.0 represents best practice and a score of 1.0 represents serious deficiencies.

Audit Area	Audit Scope	Rating
External Penetration Testing	• 1 External Perimeter • Ashburn, VA • Up to 148 IPs	4.0

Overall, Meridian scored an average 4.0 out of a possible 4.0 across the subject areas. A score of 4.0 indicates subject area meets or approaches industry best-practice. Meridian's assessment performance is notable given the scope. The strong security posture exhibited during this assessment reflects an institutional focus and priority on maintaining a robust security environment.

For The Firm,

Evan Rowell
CISSP, PCI QSA
Sr. Security Consultant
National Manager, Security Consulting
nGuard Inc.

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Meridian provides both application and network logging. Our monitoring solution monitors the network in real-time and logging tools capture details. Logging tools within the application can be used to provide audit trails which capture. For SaaS, the scope of logging tools covers the Meridian LMS application.

We track user, time, date/time, event, event details, user associated with events, and other characteristics.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Meridian LMS uses a sophisticated, yet intuitive, role based permissions architecture to restrict or grant access to data, features, and content from users and user groups. The standard demographics are the user, role, job title, organization, and custom user groups. Custom user groups work with custom fields to automate access rights (as users meet the custom characteristics, they are automatically added to their group and their access rights automatically adjust to the change). In this manner, Meridian LMS can use inbound data feeds from integrated systems to automate training assignment to only the prescribed audience (without manual intervention from admins or managers).

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Meridian defines an “information security incident” as an event – or alleged event – directed at a Client or Client(s) hosted site (herein “Site”), computers, networks, firewalls, data centers, software, data, users and services, in violation of security policies, and circumvention of security controls that could result in gaining unauthorized access, data loss, or denial/disruption of service whether the threat source is external or internal.

Examples of incidents:

- Unauthorized access or attempts to gain unauthorized access;
- Defacing of web sites;
- Installation of Malware or virus infection;
- Denial of Service attacks whether by a known or unknown perpetuator;
- Inadvertent or deliberate destruction of data;
- Unauthorized access to or theft of restricted data; and
- Malicious activities of “insider’s” with access privileges.

Meridian’s logging and monitoring tools monitor client environments in real-time and key IT personnel are notified of outages and data breaches immediately. Once a Meridian IR responder

has discovered suspicious or malicious activity involving the Client(s) site, or is notified via other sources, an incident ticket is created:

- Within one (1) minute for Severity 1 – Critical incidents
- Within thirty (30) minutes for Severity 2 – High incidents
- Within three (3) hours for Severity 3 – Medium incidents
- Within twenty-four (24) hours for Severity – 4 Low incidents

Incident Definitions

1. Critical Site is down or there is substantial inoperability to the Client(s) production system(s).
2. High Substantial degradation to the Client(s) primary production systems.
3. Medium Site is usable but an essential function is not performing to specifications. The condition impacts reasonable usage of the site. Loss of non-production systems.
4. Low Site is usable but not performing to specifications. The condition has minimal or no impact on the Client(s) ability to function.

Meridian has maintained a 99.7% availability rate (or greater) since we established our hosting SLAs. RTO is currently 96 hours and RPO is 24 hours.

Meridian's incident response plans include backup plans for Physical Communications, back up plans for Equipment and Resources, and communication escalation paths. The Employee Handbook Policy (Emergency Communications) provides a standard communication procedure to use during any emergency to communicate among employees. All employees are to be prepared and establish a plan for emergencies such as terrorism, natural disasters, severe weather, etc. A critical element of any emergency plan is communication. From the business perspective information flow is important during an emergency to let employees know what business operations are being conducted. Level and scale of the issue will dictate who communicates what information and when. Major breaches take highest priority and receive near immediate executive communication.

Email Notification

Once the Meridian Analyst has made a determination that the suspicious activity or security event under investigation is a security incident, the initial investigative ticket created is modified to escalate to the proper priority level as described above. Within each ticket and email notification the following fields may be filled out:

- Date/time of the event
- Device Alarm Description
- Incident Summary
- Synopsis of activity/alert(s) in question
- Any prior history from researching prior Atlassian JIRA tickets
- Any prior event history

- Analysis results and recommendation from the Meridian IR responder

When the ticket has been completed and escalated to the proper category:

- The Meridian IR responder drafts a Client(s) notification email and sends to the Meridian President
- Meridian President notifies Client(s) via email and/or phone with copy to the Meridian CIRT
- For Critical CAT 1 incidents, the Meridian President will contact Client(s) directly in addition to the Meridian CIRT to expedite the notification process

Contact information for the Meridian CIRT can be found in Attachment C. The incident response form will be filled out as follows:

- The Meridian IR responder will fill out as much of the required information as they know, including whether PII and/or PHI was involved. When the file contains sensitive information, such as an IP address or an account and password, this file is password protected.
- The form will then be reviewed by the Meridian Director of Information Technology and Hosting Operations and attached to the Client(s) notification email.

All correspondence related to the incident ticket will be documented and tracked within the Atlassian JIRA ticketing system.

Reporting Incidents

If a Client(s) notices any suspicious or questionable activities that result in a security incident, the Client(s) should report incidents to the Meridian Director of Information Technology and Hosting Operations. If that person is unavailable, the Client(s) may contact anyone listed in Attachment C.

Meridian Director of Information Technology and Hosting Operations can be reached via phone at (703) 261-7272.

When contacting the Meridian Director of Information Technology and Hosting Operations, Client(s) should include as much information as possible. This information should cover, but is not limited to the following:

- Exhibited Site Impact / Effect (Users can’t log in, systems performance degradation; missing or improperly formatted pages and or functionality)
- Source and Destination IP
- Date and time that event was noticed
- Source and Destination Port
- Summary of the issue
- As much descriptive detail as possible that is known at the time
- Points of contact information

Upon reporting, the Meridian Director of Information Technology and Hosting Operations will send an email notification of receipt and include an incident ticket number for reference and

tracking. Details of reporting incidents to the Meridian Director of Information Technology and Hosting Operations include:

- Notification must take place within one (1) hour of suspecting/confirming an incident has occurred or as reasonably practical.
- Notification must take place within fifteen (15) minutes of suspecting/confirming an incident involving PII and/or PHI has occurred or a reasonably practical.
- The Meridian Director of Information Technology and Hosting Operations will apprise Client(s) of response activities performed/completed throughout duration of the incident or until incident report closure.

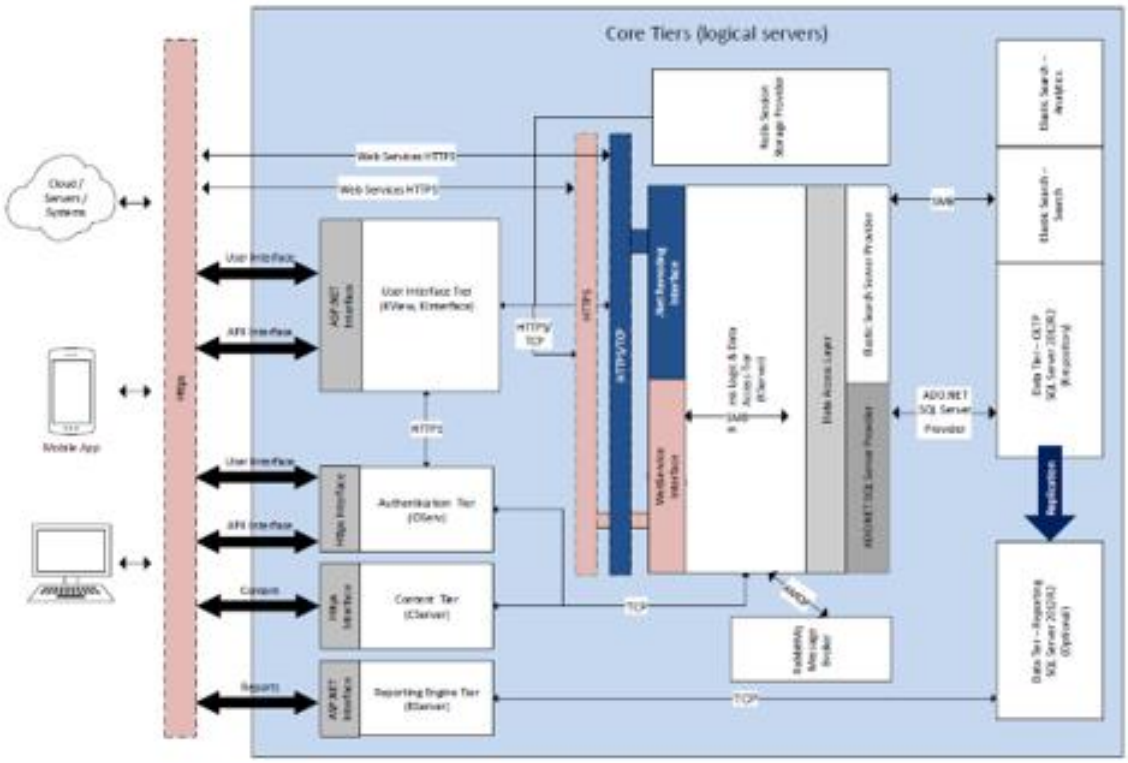
8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Meridian LMS runs in three specific zones. NIST and Zones of Control are provided via our practice with the federal government which often requires a DMZ, an app layer, and a database layer as separate zones. The separate zones prevent single calls to the databases. Our three-tier model meets this requirement. Communication is terminated and new communication is operated between each zone to ensure a single call cannot compromise the database.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

Meridian has provided a High-Level Architecture (HLA) diagram below:

Figure 3: Meridian High-Level Application Architecture



8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Part of VIP's and Meridian's recruiting and employment methodology is to conduct reference checks and background investigations. New hire documents contain verbiage that authorizes us to thoroughly investigate references, work records, education, certifications, and other matters related to the candidate's suitability for employment, continued employment and promotion. VIP and Meridian may require employee background/reference checks during the course of employment. During the course of employment, employees shall be required to report to Human Resources any criminal convictions within five (5) business days of the conviction.

VIP currently utilizes a third-party vendor to provide standardized and unbiased reference checks. Employees/applicants have rights if an adverse action is taken against hiring or promotion based on a background investigation and/or reference check.

Access to customer data is tightly controlled. Normal staff do not have access to customer systems or data contained within them. A small group of key operations support staff, do have access to customer data and systems as it is required for ongoing support, operation, and backup of the Meridian LMS.

There are times when elevated access as read-only (or with write-access) may be needed by another team member to maintain, troubleshoot, or resolve issues related to customer production (or lower environment) systems. If this need arises, a detailed request including the type of access and duration needed must be submitted for approval. Elevated access requests are reviewed and only approved on a need-to-have basis. Once elevated access is granted, it will be available for the time specified and only for the customer (and environments) for which it was approved.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

To ensure the privacy and security of your data, Meridian uses HTTPS for all communication and encrypts all inbound and outbound traffic using 128-bit and 256-bit TLS.

When data is transmitted to Meridian LMS, it first passes through the User Interface (UI) tier. Meridian LMS does not use any plug-ins that could potentially compromise security. Actions taken through the UI tier request data from, and submit data to, a dedicated Business Logic (BL) tier.

The BL tier acts as an interface between the UI tier and the database tier and maintains data integrity. It is not directly accessible via the internet and interfaces directly with the UI tier. The BL tier connects to a customer's database via a Windows service account for that specific client that only has access to that customer's data. The database tier, is located securely on a sub-network behind our firewalls and only accessible through secured connections.

Operational data stored at rest in the database, like passwords, are secured using FIPS compliant cryptography which utilizes a one-way, irreversible hashing algorithm. Personally Identifiable Information (PII) data is not required or requested by Meridian LMS, however customers can leverage custom fields to add any data they choose. Adding PII to any system should be carefully thought out and done so with care.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Meridian has detailed the following actions to be performed during Incident Response.

Tier 1: Initial Determination and Reporting

Meridian Director of Information Technology and Hosting Operations Tasks:

1. Observe or receive from first responder and IR responder information about a suspicious event or an actual incident.
2. Conduct Initial investigation of traffic in question.
3. Serve as resource to the Meridian IR responder to help identify malicious traffic.
4. Containment of the affected Client(s) site using techniques appropriate to the type of incident.
    a. Meridian Director of Information Technology and Hosting Operations provides notification to the Meridian President, who in turn will make contact with the Client(s). A notification is also made to the Meridian CIRT.
    b. Meridian Director of Information Technology and Hosting Operations coordinates with all appropriate teams in order to mitigate the malicious traffic being seen, i.e. contacting the network team to have the suspicious or malicious traffic blocked at firewall and border router.
5. If a first responder or Client(s) emails or calls the Meridian Director of Information Technology and Hosting Operations about any questionable activity, the Meridian Director of Information Technology and Hosting Operations will create an investigative ticket. Based on the investigation and events taking place the Meridian Director of Information Technology and Hosting Operations will escalate the incident as needed which will determine the priority level and allotted response time that the Meridian Director of Information Technology and Hosting Operations will have to provide follow up correspondence. The response time depends on the incident priority listed in Section 2.3.

Who

First responders to incidents often include end-users who first observe and report an anomalous event or unusual behavior of a system to the Meridian Customer Care Center (herein “CCC”). If the CCC suspects a security incident Meridian CCC staff will contact the Meridian Director of Information Technology and Hosting Operations. First responders may also be those trained to analyze events suggestive of a security incident. This includes Meridian CCC Staff, a Meridian IR responder, support staff, or Client(s).

Objective

To prioritize incidents for efficient handling by first responders reporting incidents to the Meridian CCC of the suspicious activity or anomalous behavior and providing as much information as is available for the Meridian Director of Information Technology and Hosting Operations to investigate and assess the seriousness of the incident and set the timeframe for required actions.

Responsibilities

- First responders notify the Meridian CCC and provide material evidence upon “discovery”, or where possible, and/or when asked.

- Meridian CCC forwards information to the Meridian Director of Information Technology and Hosting Operations.
- The Meridian Director of Information Technology and Hosting Operations validates the reported information and determines if a security incident is occurring.
- Upon determination the Meridian Director of Information Technology and Hosting Operations will immediately open an incident ticket in the Atlassian JIRA ticketing system, accurately document the information known at that time, and set the priority.
- The Meridian Director of Information Technology and Hosting Operations will then send email notification or place phone calls to the Meridian CIRT and all other appropriate parties depending on the impact and severity of the incident.
- The Meridian Director of Information Technology and Hosting Operations will continue to investigate, to collect and record all relevant log events, identifying the threat source, network, systems, applications or software, or individuals involved, and further assess the nature and the scope of the incident.
- The Meridian President will notify Client(s) and will provide status feedback to Client(s).

Tier 2: Follow-up, Data Collection and Restoration

Meridian Director of Information Technology and Hosting Operations Tasks:

1. Coordinate with Meridian Technical teams to isolate affected systems and collect the "live-state" data from affected systems
2. Collect evidence, store securely, and record chain of custody
3. Support vulnerability, remediation, and restoration of system
4. Assist responder team with returning systems to service
5. Notify Client(s) through the Meridian President or designee of activities performed

Who

This step may include the following staff/teams:

- Meridian Director of Information Technology and Hosting Operations
- Meridian President
- Meridian CIRT members
- Client(s)

Objectives

To ensure the handling of every incident is carried out to completion and is documented to closure.

Responsibilities

- The Meridian Director of Information Technology and Hosting Operations must facilitate quick and effective response and recovery.
- The Meridian Director of Information Technology and Hosting Operations and the Meridian Vice President, Product will make the decision regarding the need for isolation of

the system from the rest of the network, based on the seriousness of the incident and the criticality of the system.

- The Meridian Director of Information Technology and Hosting Operations coordinates and supports the Client(s) with data and evidence collection efforts, as needed.

Tier 3: Investigation and Counteraction

A member of the Meridian CIRT will coordinate with the end Client(s) their incident reporting to Government Agencies with jurisdictional responsibilities related to these events, external law enforcement, as necessary, and may decide to conduct further investigation into the incident through the gathering of additional information. In all cases the Meridian CIRT will coordinate with the Client(s) as to who will be responsible for any notifications to Government Agencies or Individuals.

Client(s) Response Tasks:

1. Collection of data for investigation and analysis. Upon request, Client(s) will be provided:
    a. Virtual Machine (herein "VM") images of the Client(s) site virtual servers to allow Client(s) to re-create incidents. Release by Meridian of a VM is available once an incident has been deemed critical, has been specifically requested by the Client and has been approved the Meridian CIRT
    b. Client(s) site server and/or network logs for incident investigation purposes

Meridian Response Tasks:

1. Meridian will conduct detailed analysis of all available evidence.
2. Meridian will maintain contact and communication with its Client(s) throughout the entire security incident handling process. Notify Client(s) of activities performed and to be reported by the Meridian Director of Information Technology and Hosting Operations to the Client(s) for incident reporting.
3. Meridian will prepare a post-mortem report that provides detailed description of the incident including:
    a. damage to Client(s) site and/or Client(s) data
    b. summary of attackers' methodology
    c. vulnerabilities exploited
    d. remedial actions
    e. proposed preventive actions

Who

All Client(s) site security incidents are initially handled by the Meridian CIRT members. Client(s) may decide to investigate the incident, in which case Meridian will support this investigation by providing relevant information in accordance with the above guidelines.

Objectives

To understand the enabling factors, cause, and effect of the security incident by performing a thorough investigation with post-mortem review to evaluate options for courses of action to prevent future incidents and enhance security controls.

Responsibilities

- The Meridian Director of Information Technology and Hosting Operations conducts the investigation of the incident and its consequences, and secures evidence so that a defensible investigation is possible.
- Client(s) attain copies of site VMs in order to conduct a separate incident analysis. Copies of Client VM instances are available provided the following guidelines are adhered to:
  - The incident at hand must be considered critical, impactful to the Client with a severe impact on the Client's business. Internal testing, development or quality assurance data will not be provided.
  - Hosted data releases must be approved by the Meridian CIRT.
  - An image file will be real time or as of the last known backup (twenty-four hours).
  - An official request must be made by the Client. The Client representative making the request must have signatory authority for the Client entity making the request. This individual must have the authority to bind the Client entity contractually.

6.2.7 (E) Migration and Redeployment Plan (8.7)

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

When a client tear down notice is received, the following occurs:

- Customer sites in all environments (Dev, QA, Stage, PreProd, Production) are deleted
- Content from production site is sent for one last backup to tape
- Database from production site is sent for one last backup to tape

These last backups and all previous backups are retained for one (1) year from date of backup, until the tape is overwritten. Backups are encrypted as they are written to tape. Backups sent to AWS will be deleted within one (1) week.

In most cases, clients are interested in migrating their data to another provider. We discuss with the client making their content and database available via SFTP so they can download and utilize with their new provider. After confirmation of download, the data is deleted from the location where it was being stored for SFTP download.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

Meridian will provide, upon request, a copy of the client database and information confirming the destruction of their back up data. Additionally, clients may export data from the database using reporting tools.

6.2.8 (E) Service or Data Recovery (8.8)

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

b. Suffers an unrecoverable loss of data.

c. Offeror experiences a system failure.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

As a part of Meridian's approach to risk management, we have developed and maintain a Contingency Recovery Plan and a Disaster Recovery Plan to ensure continuity of critical business operations and client-hosted solutions. These plans are reviewed and updated on a regular basis. The purpose of the Contingency Recovery Plan is to ensure that all critical operations can resume or continue normal processing after a software, hardware, or total site failure. All major incidents that impact SLA's are immediately addressed and communicated to the Customer Care Center and Project Manager for client notification. Meridian is committed to providing our hosted customers a highly available environment that consistently surpasses our standard SLA's for uptime. In the unfortunate event of an outage, Meridian has implemented both an internal and external monitoring solution that will immediately notify our team if a customer site or service becomes unavailable or unresponsive. Notification will also go out to our 24/7 Customer Care Center who will in-turn enter a severity ticket and begin gathering data related to the outage. If the resolution time is at risk of falling outside of our contractual SLA, the Customer Care Center will provide the client with continuous updates until resolution is achieved. Our existing Recovery Time Objective (RTO) is set to 96 hours, with a Recovery Point Objective (RPO) of up to 24 hours

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

b. Method of server image backups

c. Digital location of backup storage (secondary storage, tape, etc.)

d. Alternate data center strategies for primary data centers within the continental United States.

Meridian's backup process blends multiple types of backup software and hardware to ensure the reliability of our backups. These systems build redundancy to our backup plan and ensure that a recent backup is always available, in the event it's ever needed for recovery.

Meridian's backup process includes:

- Nightly Reverse Incremental Backups of all Production Virtual Machines

- Nightly Full Database Backups and 15 Minute Log Shipping
- Nightly Offsite Encrypted and Secure Transfers to a private Amazon Web Services Virtual Tape Library
- As part of our backup procedures, Meridian executes a daily verification checklist. Meridian utilizes automated systems and notifications to assist in the verification of backups; however, a member of our operations team also does a manual verification each day to ensure backups are valid.
- Meridian leverages the services of AWS for secure offsite backup storage. Backup data is encrypted and securely transferred from Meridian's to the US East Region and multiple availability zones on a nightly basis. Backups are stored using both S3 and Glacier Amazon services as part of the Virtual Tape Library offering.
- Customer backup data is also kept for thirty (30) days onsite for quick access in the rare event that it is needed for immediate recovery.

6.2.9 (E) Data Protection (8.9)

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

To ensure the privacy and security of your data, Meridian uses HTTPS for all communication and encrypts all inbound and outbound traffic using 128-bit and 256-bit TLS.

When data is transmitted to Meridian LMS, it first passes through the User Interface (UI) tier. Meridian LMS does not use any plug-ins that could potentially compromise security. Actions taken through the UI tier request data from, and submit data to, a dedicated Business Logic (BL) tier.

The BL tier acts as an interface between the UI tier and the database tier and maintains data integrity. It is not directly accessible via the internet and interfaces directly with the UI tier. The BL tier connects to a customer's database via a Windows service account for that specific client that only has access to that customer's data. The database tier, is located securely on a sub-network behind our firewalls and only accessible through secured connections.

Operational data stored at rest in the database, like passwords, are secured using FIPS compliant cryptography which utilizes a one-way, irreversible hashing algorithm. Personally Identifiable Information (PII) data is not required or requested by Meridian LMS, however customers can leverage custom fields to add any data they choose. Adding PII to any system should be carefully thought out and done so with care.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Meridian is compliant with this requirement and is willing to sign relevant and applicable Business Associate Agreement or other agreement mutually negotiated in good faith.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data

mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Meridian complies with this requirement. Meridian does not claim ownership to client data, and we do not use client data for purposes outside what is specified in the Master Agreement, addendums, or related service level agreement. Meridian does not resell client data, nor do we use subcontractors that would sell client data (we provide in-house services and generally do not use subcontractors without client approval).

6.2.10 (E) Service Level Agreements (8.10)

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Meridian LMS SaaS clients are hosted in the cloud with a 99.7% availability guarantee. Our Service Level Agreement is negotiable if the requested changes are attainable and reasonable.

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Service Level Agreements: **Software Support, Software Availability and Maintenance**
The Services provided by MERIDIAN under this agreement are bound by the Service Level Agreement (SLA) as described herein. In the case of an SLA violation, the respective remedies described herein will apply. The SLA penalty applicable in any given month is subject to a total cumulative penalty cap of 10% of the current month's hosting service fees ("Service Credits"). Any Service Credits due under this agreement will be credited promptly but in no event later than the quarter following the calculation of the Service Credit.

MERIDIAN will be provided a ramp up period of ninety (90) days from software Go Live (Production go live date) before any SLA requirements and subsequent remedies go into effect.

System Availability: will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time (measured in minutes) during such month, and thereafter dividing the difference so obtained by the total time during such month. Represented algebraically, System Availability for any particular calendar month is determined as follows:

$$\text{System Availability} = \frac{\text{(Total Monthly Time – Unscheduled Downtime)}}{\text{Total Monthly Time}}$$

Note: "Total Monthly Time" is deemed to include all minutes in the relevant calendar month excluding minutes of downtime caused by Scheduled Downtime, only to the extent such minutes are included within the Subscription Agreement Term.
MERIDIAN will undertake commercially reasonable measures to ensure that System Availability equals or exceeds 99.70 % during each calendar month.

a. **Measurement and Reports:** MERIDIAN will monitor System Availability metrics on an ongoing basis. All measurements of System Availability will be calculated on a monthly basis for each calendar month during the term of this agreement. MERIDIAN shall provide the System Availability report to PURCHASING ENTITY, on an as required basis, when requested by PURCHASING ENTITY. This report will contain performance metrics against the System Availability SLA obligations as depicted herein; and specific to unscheduled downtime events only.

b. **Remedies:** In the event System Availability is not equal to or greater than 99.70% for a given month, PURCHASING ENTITY will be entitled to service level credits against its subsequent payment obligations (as set forth in this Subscription Agreement) according to the following:

System Availability	**Available Credit** *(% of monthly service fee)*
99.70% - 100.00%	No Credit.
95.00% - 99.69%	Three percent (3%) of the applicable monthly hosted service fees for the applicable calendar month.
90.00% - 94.99%	Six percent (6%) of the applicable monthly hosted service fees for the applicable calendar month.
<89.99%	Ten percent (10%) of the applicable monthly hosted service fees for the applicable calendar month.

PURCHASING ENTITY's credits under this section are PURCHASING ENTITY's sole and exclusive remedy with respect to any Unscheduled Downtime or any failure by MERIDIAN to meet the Service Availability required by this agreement. The monthly available credit is capped at the lesser of $5,000 or the total cap as set forth in the System Availability section herein.

MERIDIAN will exercise commercially reasonable efforts to initiate remedial activity within two (2) hours of PURCHASING ENTITY reporting the unscheduled downtime to MERIDIAN.

c. **Exceptions**

PURCHASING ENTITY shall not receive any credits in connection with any failure or deficiency Availability caused by or associated with:

i. Force Majeure events beyond MERIDIAN's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, ecommerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this Schedule;

ii. Failure of access circuits to the ISP Network, unless such failure is caused solely by MERIDIAN;

iii. Scheduled maintenance and emergency maintenance and upgrades;

iv. DNS issues outside the direct control of MERIDIAN;
v. Issues with FTP, POP, or SMTP PURCHASING ENTITY access;
vi. False Schedule breaches reported as a result of outages or errors of any MERIDIAN measurement system;
vii. PURCHASING ENTITY's acts or omissions (or acts or omissions of others engaged or authorized by PURCHASING ENTITY), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP), any negligence, willful misconduct, or use of the Services in breach of MERIDIAN's Terms and Conditions and Acceptable Use Policy;
viii. E-mail or webmail delivery and transmission;
ix. DNS (Domain Name Server) Propagation; and / or
x. Outages elsewhere on the Internet that hinder access to your account. MERIDIAN is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. MERIDIAN will guarantee only those areas considered under the control of MERIDIAN: MERIDIAN server links to the Internet, MERIDIAN'S routers, and MERIDIAN'S servers.

d. **Software Support**

MERIDIAN will apply service packs, improvements, and enhancements as they are released to the Subscription platform. MERIDIAN will provide PURCHASING ENTITY with access to the Customer So

i. Up to five (5) named system administrators will receive access the CCC and MERIDIAN's web-based customer support portal.
ii. Notification of and access to Updates in base product format that MERIDIAN makes generally available to its Clients who have paid a maintenance support fee. Modifications to base format Updates as a result of PURCHASING ENTITY specific enhancements and integrations or installation support of Updates is not included as part of Standard Maintenance. Upon receipt of an Update by PURCHASING ENTITY, such Update will be deemed to be part of the Software for all purposes of the License Agreement.
iii. Help desk support and guidance on the use of existing base product functions. Effort exceeding a total of one (1) hour per one function is considered Training and is not included as part of Standard Maintenance Support.
iv. Troubleshooting issues associated with base product functions. If a base bug is identified, the CCC will report it to the Meridian Product team. If the issue falls within the scope of the Limited Warranty set forth in the Software License Agreement, the terms of the Limited Warranty shall apply. Base bug resolution is managed by the Meridian Product team. Determination of the need and prioritization of Updates to address reported issues outside of the scope of the Limited Warranty is at the sole discretion of MERIDIAN, and this Exhibit C-1 shall not be construed as an addition or change to the terms set forth in the Limited Warranty of the Agreement.
v. CCC Support Hours can be provided during standard business hours or 24/7. PURCHASING ENTITY support hours are as defined in the table below:

CCC Support Hours (Selection Marked with "X")		
X	Standard	Standard business days only, from 8am to 8pm Eastern Time by telephone and/or Meridian support portal
	Extended	24/7 access by telephone or Meridian support portal

The Client acknowledges from time to time in Company's sole discretion but using commercially reasonable efforts to minimize any disruption of the Service, MERIDIAN will schedule standard system maintenance, including version upgrades to the Software and/or system, in which case MERIDIAN will announce the scheduled maintenance via e-mail to PURCHASING ENTITY's designated e-mail address.

e. **Software Support Severity Level Definitions**

All reported issues to the CCC will be assigned a Severity Level which defines the critical nature of the problem. The Severity Level will drive CCC response to the PURCHASING ENTITY, internal escalation process, on procedures per a defined timeline.

The following table defines the four (4) standard Severity Levels that will be assigned to MERIDIAN documented issues. Subsequent tables outline the notification and escalation processes for each defined Severity Level.

Severity Level	Severity Description	Response Time
1 Critical	Issue that causes complete loss of service to the PURCHASING ENTITY's production environment and work cannot reasonably continue. Workarounds to provide the same functionality are not possible and cannot be found in time to minimize the impact on the PURCHASING ENTITY's business. The problem has one or more of the following characteristics: Fifty percent of users cannot access the system. Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, loss of functionality that is financially impacting. Severe performance degradation rendering the system unusable. Loss of data that cannot be reasonably retrieved. Security vulnerabilities that could expose PII data.	One (1) Hour
2 Major	Issue where operation of the system is considered severely limited, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics: A software error for which there is a Customer acceptable workaround. Self-contained issue that does not impact the overall functionality of the software. Minimal performance degradation which impacts productivity.	One (1) business day

3 Minor	Issue that causes no loss of service and in no way impedes use of the system. The problem has one or more of the following characteristics: Guidance on the use of existing base product functions and Customer accepted modifications. Cosmetic issue such as misspelled words or misaligned text. Enhancement requests to update functionality.	Two (2) business days
4 Minimal	Questions regarding system functionality where product user guides are confusing or non- existent and answers are limited to under thirty (30) minutes.	Three (3) business days

PURCHASING ENTITY Responsibilities: To provide effective support, additional information may be required by PURCHASING ENTITY. Additional details regarding MERIDIAN and PURCHASING ENTITY responsibilities are documented in the MERIDIAN Customer Support Policy.

f. Support Exclusions.

The following services are not included Support, but can be provided as separate, optional tasks:

i. Training on Software functions and modifications in excess of standard help desk support. Training shall be defined as one or more discussions about one function within the Software, where the total discussion time exceeds one (1) hour.

ii. End User support, or support to any person other than the five named administrators.

iii. Troubleshooting or resolution of hardware, software, security, or network-related issues on PURCHASING ENTITY servers or workstations.

iv. Project management support, including administration of PURCHASING ENTITY funding and project reports to PURCHASING ENTITY.

v. Courseware support, including loading of content into the site, troubleshooting issues with third party or client developed courseware, or troubleshooting user or browser configuration or related issues with viewing courseware.

vi. Integration with PURCHASING ENTITY applications (such as Active Directory, HRIS, or others).

g. **Credit Request and Payment Procedures.**

In order to receive a credit for system availability as defined in Section 28b herein, PURCHASING ENTITY must make a request therefore by sending an email message to creditrequest@meridianks.com. Each request in connection with this Schedule must include PURCHASING ENTITY’s account number (per MERIDIAN’s invoice) and the dates and times of the unavailability of PURCHASING ENTITY's Web site and must be received by MERIDIAN within ten (10) business days after PURCHASING ENTITY's Web Site was not available. If the unavailability is confirmed by MERIDIAN, credits will be applied within one week after MERIDIAN's receipt of PURCHASING ENTITY's credit request.

Notwithstanding anything to the contrary herein, the total amount credited to PURCHASING ENTITY in a particular month under this Service Level Agreement shall not exceed the total Subscription fee paid by PURCHASING ENTITY for such month for the affected Services. Credits are exclusive of any

applicable taxes charged to PURCHASING ENTITY or collected by MERIDIAN and are PURCHASING ENTITY's sole and exclusive remedy with respect to any failure or deficiency in the Availability of Service.

6.2.11 (E) Data Disposal (8.11)

Specify your data disposal procedures and policies and destruction confirmation process.

Meridian follows industry best practices for data destruction policies. We use AWS Eastern Region as our backup storage location and we follow their best practices for data destruction and disposal methods.

6.2.12 (E) Performance Measures And Reporting (8.12)

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Meridian's guaranteed SLA is 99.7% availability and we typically achieve availability of 98% or higher.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

Service Level Agreements: **Software Support, Software Availability and Maintenance**
The Services provided by MERIDIAN under this agreement are bound by the Service Level Agreement (SLA) as described herein. In the case of an SLA violation, the respective remedies described herein will apply. The SLA penalty applicable in any given month is subject to a total cumulative penalty cap of 10% of the current month's hosting service fees ("Service Credits"). Any Service Credits due under this agreement will be credited promptly but in no event later than the quarter following the calculation of the Service Credit.

MERIDIAN will be provided a ramp up period of ninety (90) days from software Go Live (Production go live date) before any SLA requirements and subsequent remedies go into effect.

System Availability: will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time (measured in minutes) during such month, and thereafter dividing the difference so obtained by the total time during such month. Represented algebraically, System Availability for any particular calendar month is determined as follows:

$$\text{System Availability} = \frac{\text{(Total Monthly Time – Unscheduled Downtime)}}{\text{Total Monthly Time}}$$

Note: "Total Monthly Time" is deemed to include all minutes in the relevant calendar month excluding minutes of downtime caused by Scheduled Downtime, only to the extent such minutes are included within the Subscription Agreement Term.
MERIDIAN will undertake commercially reasonable measures to ensure that System Availability equals or exceeds 99.70 % during each calendar month.

a. **Measurement and Reports:** MERIDIAN will monitor System Availability metrics on an ongoing basis. All measurements of System Availability will be calculated on a monthly basis for each calendar month during the term of this agreement. MERIDIAN shall provide the System Availability report to PURCHASING ENTITY, on an as required basis, when requested by PURCHASING ENTITY. This report will contain performance metrics against the System Availability SLA obligations as depicted herein; and specific to unscheduled downtime events only.

b. **Remedies:** In the event System Availability is not equal to or greater than 99.70% for a given month, PURCHASING ENTITY will be entitled to service level credits against its subsequent payment obligations (as set forth in this Subscription Agreement) according to the following:

System Availability	**Available Credit** *(% of monthly service fee)*
99.70% - 100.00%	No Credit.
95.00% - 99.69%	Three percent (3%) of the applicable monthly hosted service fees for the applicable calendar month.
90.00% - 94.99%	Six percent (6%) of the applicable monthly hosted service fees for the applicable calendar month.
<89.99%	Ten percent (10%) of the applicable monthly hosted service fees for the applicable calendar month.

PURCHASING ENTITY's credits under this section are PURCHASING ENTITY's sole and exclusive remedy with respect to any Unscheduled Downtime or any failure by MERIDIAN to meet the Service Availability required by this agreement. The monthly available credit is capped at the lesser of $5,000 or the total cap as set forth in the System Availability section herein.

MERIDIAN will exercise commercially reasonable efforts to initiate remedial activity within two (2) hours of PURCHASING ENTITY reporting the unscheduled downtime to MERIDIAN.

c. **Exceptions**

PURCHASING ENTITY shall not receive any credits in connection with any failure or deficiency Availability caused by or associated with:

i. Force Majeure events beyond MERIDIAN's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, ecommerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this Schedule;

ii. Failure of access circuits to the ISP Network, unless such failure is caused solely by MERIDIAN;

iii. Scheduled maintenance and emergency maintenance and upgrades;

iv. DNS issues outside the direct control of MERIDIAN;
v. Issues with FTP, POP, or SMTP PURCHASING ENTITY access;
vi. False Schedule breaches reported as a result of outages or errors of any MERIDIAN measurement system;
vii. PURCHASING ENTITY's acts or omissions (or acts or omissions of others engaged or authorized by PURCHASING ENTITY), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP), any negligence, willful misconduct, or use of the Services in breach of MERIDIAN's Terms and Conditions and Acceptable Use Policy;
viii. E-mail or webmail delivery and transmission;
ix. DNS (Domain Name Server) Propagation; and / or
x. Outages elsewhere on the Internet that hinder access to your account. MERIDIAN is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. MERIDIAN will guarantee only those areas considered under the control of MERIDIAN: MERIDIAN server links to the Internet, MERIDIAN'S routers, and MERIDIAN'S servers.

d. **Software Support**

MERIDIAN will apply service packs, improvements, and enhancements as they are released to the Subscription platform. MERIDIAN will provide PURCHASING ENTITY with access to the Customer So

i. Up to five (5) named system administrators will receive access the CCC and MERIDIAN's web-based customer support portal.
ii. Notification of and access to Updates in base product format that MERIDIAN makes generally available to its Clients who have paid a maintenance support fee. Modifications to base format Updates as a result of PURCHASING ENTITY specific enhancements and integrations or installation support of Updates is not included as part of Standard Maintenance. Upon receipt of an Update by PURCHASING ENTITY, such Update will be deemed to be part of the Software for all purposes of the License Agreement.
iii. Help desk support and guidance on the use of existing base product functions. Effort exceeding a total of one (1) hour per one function is considered Training and is not included as part of Standard Maintenance Support.
iv. Troubleshooting issues associated with base product functions. If a base bug is identified, the CCC will report it to the Meridian Product team. If the issue falls within the scope of the Limited Warranty set forth in the Software License Agreement, the terms of the Limited Warranty shall apply. Base bug resolution is managed by the Meridian Product team. Determination of the need and prioritization of Updates to address reported issues outside of the scope of the Limited Warranty is at the sole discretion of MERIDIAN, and this Exhibit C-1 shall not be construed as an addition or change to the terms set forth in the Limited Warranty of the Agreement.
v. CCC Support Hours can be provided during standard business hours or 24/7. PURCHASING ENTITY support hours are as defined in the table below:

CCC Support Hours (Selection Marked with "X")		
X	Standard	Standard business days only, from 8am to 8pm Eastern Time by telephone and/or Meridian support portal
	Extended	24/7 access by telephone or Meridian support portal

The Client acknowledges from time to time in Company's sole discretion but using commercially reasonable efforts to minimize any disruption of the Service, MERIDIAN will schedule standard system maintenance, including version upgrades to the Software and/or system, in which case MERIDIAN will announce the scheduled maintenance via e-mail to PURCHASING ENTITY's designated e-mail address.

e. **Software Support Severity Level Definitions**

All reported issues to the CCC will be assigned a Severity Level which defines the critical nature of the problem. The Severity Level will drive CCC response to the PURCHASING ENTITY, internal escalation process, on procedures per a defined timeline.

The following table defines the four (4) standard Severity Levels that will be assigned to MERIDIAN documented issues. Subsequent tables outline the notification and escalation processes for each defined Severity Level.

Severity Level	Severity Description	Response Time
1 Critical	Issue that causes complete loss of service to the PURCHASING ENTITY's production environment and work cannot reasonably continue. Workarounds to provide the same functionality are not possible and cannot be found in time to minimize the impact on the PURCHASING ENTITY's business. The problem has one or more of the following characteristics: Fifty percent of users cannot access the system. Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, loss of functionality that is financially impacting. Severe performance degradation rendering the system unusable. Loss of data that cannot be reasonably retrieved. Security vulnerabilities that could expose PII data.	One (1) Hour
2 Major	Issue where operation of the system is considered severely limited, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics: A software error for which there is a Customer acceptable workaround. Self-contained issue that does not impact the overall functionality of the software. Minimal performance degradation which impacts productivity.	One (1) business day

3 Minor	Issue that causes no loss of service and in no way impedes use of the system. The problem has one or more of the following characteristics: Guidance on the use of existing base product functions and Customer accepted modifications. Cosmetic issue such as misspelled words or misaligned text. Enhancement requests to update functionality.	Two (2) business days
4 Minimal	Questions regarding system functionality where product user guides are confusing or non- existent and answers are limited to under thirty (30) minutes.	Three (3) business days

PURCHASING ENTITY Responsibilities: To provide effective support, additional information may be required by PURCHASING ENTITY. Additional details regarding MERIDIAN and PURCHASING ENTITY responsibilities are documented in the MERIDIAN Customer Support Policy.

f. Support Exclusions.

The following services are not included Support, but can be provided as separate, optional tasks:

i. Training on Software functions and modifications in excess of standard help desk support. Training shall be defined as one or more discussions about one function within the Software, where the total discussion time exceeds one (1) hour.

ii. End User support, or support to any person other than the five named administrators.

iii. Troubleshooting or resolution of hardware, software, security, or network-related issues on PURCHASING ENTITY servers or workstations.

iv. Project management support, including administration of PURCHASING ENTITY funding and project reports to PURCHASING ENTITY.

v. Courseware support, including loading of content into the site, troubleshooting issues with third party or client developed courseware, or troubleshooting user or browser configuration or related issues with viewing courseware.

vi. Integration with PURCHASING ENTITY applications (such as Active Directory, HRIS, or others).

g. **Credit Request and Payment Procedures.**

In order to receive a credit for system availability as defined in Section 28b herein, PURCHASING ENTITY must make a request therefore by sending an email message to creditrequest@meridianks.com. Each request in connection with this Schedule must include PURCHASING ENTITY’s account number (per MERIDIAN’s invoice) and the dates and times of the unavailability of PURCHASING ENTITY's Web site and must be received by MERIDIAN within ten (10) business days after PURCHASING ENTITY's Web Site was not available. If the unavailability is confirmed by MERIDIAN, credits will be applied within one week after MERIDIAN's receipt of PURCHASING ENTITY's credit request.

Notwithstanding anything to the contrary herein, the total amount credited to PURCHASING ENTITY in a particular month under this Service Level Agreement shall not exceed the total Subscription fee paid by PURCHASING ENTITY for such month for the affected Services. Credits are exclusive of any

applicable taxes charged to PURCHASING ENTITY or collected by MERIDIAN and are PURCHASING ENTITY's sole and exclusive remedy with respect to any failure or deficiency in the Availability of Service.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

Meridian support is available via our in-house Customer Care Center in Reston, Virginia. Support requests can be processed by phone, ticket, or support portal. Once the request is processed, it is triaged by the CCC team according to severity. Each level of severity has a corresponding SLA for response time and escalation procedures and paths. Support tickets may be submitted 24x7 and phone support is available from 8 AM to 8 PM (EST) to cover standard business hours in all U.S. time zones. Support is provided by in-house Meridian staff and is not outsourced. Finally, each client has a customer success manager to serve as their advocate within Meridian and provide ongoing consulting on emerging trends and technologies.

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

Service Level Agreements: **Software Support, Software Availability and Maintenance**
The Services provided by MERIDIAN under this agreement are bound by the Service Level Agreement (SLA) as described herein. In the case of an SLA violation, the respective remedies described herein will apply. The SLA penalty applicable in any given month is subject to a total cumulative penalty cap of 10% of the current month's hosting service fees ("Service Credits"). Any Service Credits due under this agreement will be credited promptly but in no event later than the quarter following the calculation of the Service Credit.

MERIDIAN will be provided a ramp up period of ninety (90) days from software Go Live (Production go live date) before any SLA requirements and subsequent remedies go into effect.

System Availability: will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time (measured in minutes) during such month, and thereafter dividing the difference so obtained by the total time during such month. Represented algebraically, System Availability for any particular calendar month is determined as follows:

$$\text{System Availability} = \frac{\text{(Total Monthly Time – Unscheduled Downtime)}}{\text{Total Monthly Time}}$$

Note: "Total Monthly Time" is deemed to include all minutes in the relevant calendar month excluding minutes of downtime caused by Scheduled Downtime, only to the extent such minutes are included within the Subscription Agreement Term.
MERIDIAN will undertake commercially reasonable measures to ensure that System Availability equals or exceeds 99.70 % during each calendar month.

a. **Measurement and Reports:** MERIDIAN will monitor System Availability metrics on an ongoing basis. All measurements of System Availability will be calculated on a monthly basis for each calendar month during the term of this agreement. MERIDIAN shall provide the System Availability report to PURCHASING ENTITY, on an as required basis, when requested by PURCHASING ENTITY. This report will contain performance metrics against the System Availability SLA obligations as depicted herein; and specific to unscheduled downtime events only.

b. **Remedies:** In the event System Availability is not equal to or greater than 99.70% for a given month, PURCHASING ENTITY will be entitled to service level credits against its subsequent payment obligations (as set forth in this Subscription Agreement) according to the following:

System Availability	**Available Credit** *(% of monthly service fee)*
99.70% - 100.00%	No Credit.
95.00% - 99.69%	Three percent (3%) of the applicable monthly hosted service fees for the applicable calendar month.
90.00% - 94.99%	Six percent (6%) of the applicable monthly hosted service fees for the applicable calendar month.
<89.99%	Ten percent (10%) of the applicable monthly hosted service fees for the applicable calendar month.

PURCHASING ENTITY's credits under this section are PURCHASING ENTITY's sole and exclusive remedy with respect to any Unscheduled Downtime or any failure by MERIDIAN to meet the Service Availability required by this agreement. The monthly available credit is capped at the lesser of $5,000 or the total cap as set forth in the System Availability section herein.

MERIDIAN will exercise commercially reasonable efforts to initiate remedial activity within two (2) hours of PURCHASING ENTITY reporting the unscheduled downtime to MERIDIAN.

c. **Exceptions**

PURCHASING ENTITY shall not receive any credits in connection with any failure or deficiency Availability caused by or associated with:

i. Force Majeure events beyond MERIDIAN's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, ecommerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this Schedule;

ii. Failure of access circuits to the ISP Network, unless such failure is caused solely by MERIDIAN;

iii. Scheduled maintenance and emergency maintenance and upgrades;

iv. DNS issues outside the direct control of MERIDIAN;
v. Issues with FTP, POP, or SMTP PURCHASING ENTITY access;
vi. False Schedule breaches reported as a result of outages or errors of any MERIDIAN measurement system;
vii. PURCHASING ENTITY's acts or omissions (or acts or omissions of others engaged or authorized by PURCHASING ENTITY), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP), any negligence, willful misconduct, or use of the Services in breach of MERIDIAN's Terms and Conditions and Acceptable Use Policy;
viii. E-mail or webmail delivery and transmission;
ix. DNS (Domain Name Server) Propagation; and / or
x. Outages elsewhere on the Internet that hinder access to your account. MERIDIAN is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. MERIDIAN will guarantee only those areas considered under the control of MERIDIAN: MERIDIAN server links to the Internet, MERIDIAN'S routers, and MERIDIAN'S servers.

d. **Software Support**

MERIDIAN will apply service packs, improvements, and enhancements as they are released to the Subscription platform. MERIDIAN will provide PURCHASING ENTITY with access to the Customer So

i. Up to five (5) named system administrators will receive access the CCC and MERIDIAN's web-based customer support portal.
ii. Notification of and access to Updates in base product format that MERIDIAN makes generally available to its Clients who have paid a maintenance support fee. Modifications to base format Updates as a result of PURCHASING ENTITY specific enhancements and integrations or installation support of Updates is not included as part of Standard Maintenance. Upon receipt of an Update by PURCHASING ENTITY, such Update will be deemed to be part of the Software for all purposes of the License Agreement.
iii. Help desk support and guidance on the use of existing base product functions. Effort exceeding a total of one (1) hour per one function is considered Training and is not included as part of Standard Maintenance Support.
iv. Troubleshooting issues associated with base product functions. If a base bug is identified, the CCC will report it to the Meridian Product team. If the issue falls within the scope of the Limited Warranty set forth in the Software License Agreement, the terms of the Limited Warranty shall apply. Base bug resolution is managed by the Meridian Product team. Determination of the need and prioritization of Updates to address reported issues outside of the scope of the Limited Warranty is at the sole discretion of MERIDIAN, and this Exhibit C-1 shall not be construed as an addition or change to the terms set forth in the Limited Warranty of the Agreement.
v. CCC Support Hours can be provided during standard business hours or 24/7. PURCHASING ENTITY support hours are as defined in the table below:

CCC Support Hours (Selection Marked with "X")		
X	Standard	Standard business days only, from 8am to 8pm Eastern Time by telephone and/or Meridian support portal
	Extended	24/7 access by telephone or Meridian support portal

The Client acknowledges from time to time in Company's sole discretion but using commercially reasonable efforts to minimize any disruption of the Service, MERIDIAN will schedule standard system maintenance, including version upgrades to the Software and/or system, in which case MERIDIAN will announce the scheduled maintenance via e-mail to PURCHASING ENTITY's designated e-mail address.

e. **Software Support Severity Level Definitions**

All reported issues to the CCC will be assigned a Severity Level which defines the critical nature of the problem. The Severity Level will drive CCC response to the PURCHASING ENTITY, internal escalation process, on procedures per a defined timeline.

The following table defines the four (4) standard Severity Levels that will be assigned to MERIDIAN documented issues. Subsequent tables outline the notification and escalation processes for each defined Severity Level.

Severity Level	Severity Description	Response Time
1 Critical	Issue that causes complete loss of service to the PURCHASING ENTITY's production environment and work cannot reasonably continue. Workarounds to provide the same functionality are not possible and cannot be found in time to minimize the impact on the PURCHASING ENTITY's business. The problem has one or more of the following characteristics: Fifty percent of users cannot access the system. Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, loss of functionality that is financially impacting. Severe performance degradation rendering the system unusable. Loss of data that cannot be reasonably retrieved. Security vulnerabilities that could expose PII data.	One (1) Hour
2 Major	Issue where operation of the system is considered severely limited, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics: A software error for which there is a Customer acceptable workaround. Self-contained issue that does not impact the overall functionality of the software. Minimal performance degradation which impacts productivity.	One (1) business day

3 Minor	Issue that causes no loss of service and in no way impedes use of the system. The problem has one or more of the following characteristics: Guidance on the use of existing base product functions and Customer accepted modifications. Cosmetic issue such as misspelled words or misaligned text. Enhancement requests to update functionality.	Two (2) business days
4 Minimal	Questions regarding system functionality where product user guides are confusing or non- existent and answers are limited to under thirty (30) minutes.	Three (3) business days

PURCHASING ENTITY Responsibilities: To provide effective support, additional information may be required by PURCHASING ENTITY. Additional details regarding MERIDIAN and PURCHASING ENTITY responsibilities are documented in the MERIDIAN Customer Support Policy.

f. Support Exclusions.

The following services are not included Support, but can be provided as separate, optional tasks:

i. Training on Software functions and modifications in excess of standard help desk support. Training shall be defined as one or more discussions about one function within the Software, where the total discussion time exceeds one (1) hour.

ii. End User support, or support to any person other than the five named administrators.

iii. Troubleshooting or resolution of hardware, software, security, or network-related issues on PURCHASING ENTITY servers or workstations.

iv. Project management support, including administration of PURCHASING ENTITY funding and project reports to PURCHASING ENTITY.

v. Courseware support, including loading of content into the site, troubleshooting issues with third party or client developed courseware, or troubleshooting user or browser configuration or related issues with viewing courseware.

vi. Integration with PURCHASING ENTITY applications (such as Active Directory, HRIS, or others).

g. **Credit Request and Payment Procedures.**

In order to receive a credit for system availability as defined in Section 28b herein, PURCHASING ENTITY must make a request therefore by sending an email message to creditrequest@meridianks.com. Each request in connection with this Schedule must include PURCHASING ENTITY’s account number (per MERIDIAN’s invoice) and the dates and times of the unavailability of PURCHASING ENTITY's Web site and must be received by MERIDIAN within ten (10) business days after PURCHASING ENTITY's Web Site was not available. If the unavailability is confirmed by MERIDIAN, credits will be applied within one week after MERIDIAN's receipt of PURCHASING ENTITY's credit request.

Notwithstanding anything to the contrary herein, the total amount credited to PURCHASING ENTITY in a particular month under this Service Level Agreement shall not exceed the total Subscription fee paid by PURCHASING ENTITY for such month for the affected Services. Credits are exclusive of any

applicable taxes charged to PURCHASING ENTITY or collected by MERIDIAN and are PURCHASING ENTITY's sole and exclusive remedy with respect to any failure or deficiency in the Availability of Service.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

Meridian provides monthly maintenance for our SaaS clients (maintenance schedules are published at the beginning of each year). Downtimes are scheduled in non-business hours to minimize maintenance impact on the user base. The SaaS environment receives two upgrades per year (spring and fall) to introduce new product features. SaaS upgrade timelines are minimal and do not fall outside our 99.7% availability guarantee.

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Meridian's SLA contract language is included below.

Service Level Agreements: **Software Support, Software Availability and Maintenance**
The Services provided by MERIDIAN under this agreement are bound by the Service Level Agreement (SLA) as described herein. In the case of an SLA violation, the respective remedies described herein will apply. The SLA penalty applicable in any given month is subject to a total cumulative penalty cap of 10% of the current month's hosting service fees ("Service Credits"). Any Service Credits due under this agreement will be credited promptly but in no event later than the quarter following the calculation of the Service Credit.

MERIDIAN will be provided a ramp up period of ninety (90) days from software Go Live (Production go live date) before any SLA requirements and subsequent remedies go into effect.

System Availability: will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time (measured in minutes) during such month, and thereafter dividing the difference so obtained by the total time during such month. Represented algebraically, System Availability for any particular calendar month is determined as follows:

$$\text{System Availability} = \frac{\text{(Total Monthly Time – Unscheduled Downtime)}}{\text{Total Monthly Time}}$$

Note: "Total Monthly Time" is deemed to include all minutes in the relevant calendar month excluding minutes of downtime caused by Scheduled Downtime, only to the extent such minutes are included within the Subscription Agreement Term.
MERIDIAN will undertake commercially reasonable measures to ensure that System Availability equals or exceeds 99.70 % during each calendar month.

a. **Measurement and Reports:** MERIDIAN will monitor System Availability metrics on an ongoing basis. All measurements of System Availability will be calculated on a monthly basis for each

calendar month during the term of this agreement. MERIDIAN shall provide the System Availability report to PURCHASING ENTITY, on an as required basis, when requested by PURCHASING ENTITY. This report will contain performance metrics against the System Availability SLA obligations as depicted herein; and specific to unscheduled downtime events only.

b. **Remedies:** In the event System Availability is not equal to or greater than 99.70% for a given month, PURCHASING ENTITY will be entitled to service level credits against its subsequent payment obligations (as set forth in this Subscription Agreement) according to the following:

System Availability	Available Credit *(% of monthly service fee)*
99.70% - 100.00%	No Credit.
95.00% - 99.69%	Three percent (3%) of the applicable monthly hosted service fees for the applicable calendar month.
90.00% - 94.99%	Six percent (6%) of the applicable monthly hosted service fees for the applicable calendar month.
<89.99%	Ten percent (10%) of the applicable monthly hosted service fees for the applicable calendar month.

PURCHASING ENTITY's credits under this section are PURCHASING ENTITY's sole and exclusive remedy with respect to any Unscheduled Downtime or any failure by MERIDIAN to meet the Service Availability required by this agreement. The monthly available credit is capped at the lesser of $5,000 or the total cap as set forth in the System Availability section herein.

MERIDIAN will exercise commercially reasonable efforts to initiate remedial activity within two (2) hours of PURCHASING ENTITY reporting the unscheduled downtime to MERIDIAN.

c. **Exceptions**

PURCHASING ENTITY shall not receive any credits in connection with any failure or deficiency Availability caused by or associated with:

i. Force Majeure events beyond MERIDIAN's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, ecommerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this Schedule;

ii. Failure of access circuits to the ISP Network, unless such failure is caused solely by MERIDIAN;

iii. Scheduled maintenance and emergency maintenance and upgrades;

iv. DNS issues outside the direct control of MERIDIAN;

v. Issues with FTP, POP, or SMTP PURCHASING ENTITY access;

vi. False Schedule breaches reported as a result of outages or errors of any MERIDIAN measurement system;

vii. PURCHASING ENTITY's acts or omissions (or acts or omissions of others engaged or authorized by PURCHASING ENTITY), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP), any negligence, willful misconduct, or use of the Services in breach of MERIDIAN's Terms and Conditions and Acceptable Use Policy;

viii. E-mail or webmail delivery and transmission;

ix. DNS (Domain Name Server) Propagation; and / or

x. Outages elsewhere on the Internet that hinder access to your account. MERIDIAN is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. MERIDIAN will guarantee only those areas considered under the control of MERIDIAN: MERIDIAN server links to the Internet, MERIDIAN'S routers, and MERIDIAN'S servers.

d. **Software Support**

MERIDIAN will apply service packs, improvements, and enhancements as they are released to the Subscription platform. MERIDIAN will provide PURCHASING ENTITY with access to the Customer So

i. Up to five (5) named system administrators will receive access the CCC and MERIDIAN's web-based customer support portal.

ii. Notification of and access to Updates in base product format that MERIDIAN makes generally available to its Clients who have paid a maintenance support fee. Modifications to base format Updates as a result of PURCHASING ENTITY specific enhancements and integrations or installation support of Updates is not included as part of Standard Maintenance. Upon receipt of an Update by PURCHASING ENTITY, such Update will be deemed to be part of the Software for all purposes of the License Agreement.

iii. Help desk support and guidance on the use of existing base product functions. Effort exceeding a total of one (1) hour per one function is considered Training and is not included as part of Standard Maintenance Support.

iv. Troubleshooting issues associated with base product functions. If a base bug is identified, the CCC will report it to the Meridian Product team. If the issue falls within the scope of the Limited Warranty set forth in the Software License Agreement, the terms of the Limited Warranty shall apply. Base bug resolution is managed by the Meridian Product team. Determination of the need and prioritization of Updates to address reported issues outside of the scope of the Limited Warranty is at the sole discretion of MERIDIAN, and this Exhibit C-1 shall not be construed as an addition or change to the terms set forth in the Limited Warranty of the Agreement.

v. CCC Support Hours can be provided during standard business hours or 24/7. PURCHASING ENTITY support hours are as defined in the table below:

CCC Support Hours (Selection Marked with "X")		
X	Standard	Standard business days only, from 8am to 8pm Eastern Time by telephone and/or Meridian support portal
	Extended	24/7 access by telephone or Meridian support portal

The Client acknowledges from time to time in Company's sole discretion but using commercially reasonable efforts to minimize any disruption of the Service, MERIDIAN will schedule standard system maintenance, including version upgrades to the Software and/or system, in which case MERIDIAN will announce the scheduled maintenance via e-mail to PURCHASING ENTITY's designated e-mail address.

e. **Software Support Severity Level Definitions**

All reported issues to the CCC will be assigned a Severity Level which defines the critical nature of the problem. The Severity Level will drive CCC response to the PURCHASING ENTITY, internal escalation process, on procedures per a defined timeline.

The following table defines the four (4) standard Severity Levels that will be assigned to MERIDIAN documented issues. Subsequent tables outline the notification and escalation processes for each defined Severity Level.

Severity Level	Severity Description	Response Time
1 Critical	Issue that causes complete loss of service to the PURCHASING ENTITY's production environment and work cannot reasonably continue. Workarounds to provide the same functionality are not possible and cannot be found in time to minimize the impact on the PURCHASING ENTITY's business. The problem has one or more of the following characteristics: Fifty percent of users cannot access the system. Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, loss of functionality that is financially impacting. Severe performance degradation rendering the system unusable. Loss of data that cannot be reasonably retrieved. Security vulnerabilities that could expose PII data.	One (1) Hour
2 Major	Issue where operation of the system is considered severely limited, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics: A software error for which there is a Customer acceptable workaround. Self-contained issue that does not impact the overall functionality of the software. Minimal performance degradation which impacts productivity.	One (1) business day

3 Minor	Issue that causes no loss of service and in no way impedes use of the system. The problem has one or more of the following characteristics: Guidance on the use of existing base product functions and Customer accepted modifications. Cosmetic issue such as misspelled words or misaligned text. Enhancement requests to update functionality.	Two (2) business days
4 Minimal	Questions regarding system functionality where product user guides are confusing or non- existent and answers are limited to under thirty (30) minutes.	Three (3) business days

PURCHASING ENTITY Responsibilities: To provide effective support, additional information may be required by PURCHASING ENTITY. Additional details regarding MERIDIAN and PURCHASING ENTITY responsibilities are documented in the MERIDIAN Customer Support Policy.

f. Support Exclusions.

The following services are not included Support, but can be provided as separate, optional tasks:

i. Training on Software functions and modifications in excess of standard help desk support. Training shall be defined as one or more discussions about one function within the Software, where the total discussion time exceeds one (1) hour.

ii. End User support, or support to any person other than the five named administrators.

iii. Troubleshooting or resolution of hardware, software, security, or network-related issues on PURCHASING ENTITY servers or workstations.

iv. Project management support, including administration of PURCHASING ENTITY funding and project reports to PURCHASING ENTITY.

v. Courseware support, including loading of content into the site, troubleshooting issues with third party or client developed courseware, or troubleshooting user or browser configuration or related issues with viewing courseware.

vi. Integration with PURCHASING ENTITY applications (such as Active Directory, HRIS, or others).

g. **Credit Request and Payment Procedures.**

In order to receive a credit for system availability as defined in Section 28b herein, PURCHASING ENTITY must make a request therefore by sending an email message to creditrequest@meridianks.com. Each request in connection with this Schedule must include PURCHASING ENTITY’s account number (per MERIDIAN’s invoice) and the dates and times of the unavailability of PURCHASING ENTITY's Web site and must be received by MERIDIAN within ten (10) business days after PURCHASING ENTITY's Web Site was not available. If the unavailability is confirmed by MERIDIAN, credits will be applied within one week after MERIDIAN's receipt of PURCHASING ENTITY's credit request.

Notwithstanding anything to the contrary herein, the total amount credited to PURCHASING ENTITY in a particular month under this Service Level Agreement shall not exceed the total Subscription fee paid by PURCHASING ENTITY for such month for the affected Services. Credits are exclusive of any

applicable taxes charged to PURCHASING ENTITY or collected by MERIDIAN and are PURCHASING ENTITY's sole and exclusive remedy with respect to any failure or deficiency in the Availability of Service.

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

A sample performance report is provided in Document 6: Appendix A. 8.12.8 Ability to print historical, statistical, and usage reports locally.

Yes, we can go back three (3) years or more even on these types of reports. All SLA reports are tested externally but RAM and CPU type reports are local (Solarwinds monitoring).

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

Meridian's network operations center is supported 24x365.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Network scalability can be increased or decreased as required. Critical server issues are addressed 24x365. Meridian monitors and scales as required.

From an application perspective, Meridian LMS is a multi-tiered application built upon the .NET framework and designed from the ground up with scalability in mind. Each of the application tiers of the can be scaled up or down to meet customer demand.

While Meridian LMS is not bandwidth intensive, the content customers make available to their users can be. It is important that content types and delivery methods are examined to ensure that they can be accessed by a customer's user base.

To help ensure Meridian LMS and any uploaded content can be accessed efficiently by users distributed across the globe, Meridian also offers Content Delivery Network (or CDN) services. The CDN utilize caching and traffic acceleration techniques that have proven to decrease round-trips to Meridian LMS origin servers, reduce the number of ISP hops for users, increase overall download/transfer speeds, and improve overall LMS site performance.

In many cases, high levels of user concurrency will be required of the Meridian LMS due to the nature of customer's seasonal training needs. Meridian has the expertise necessary to provide our clients a secure, scalable LMS solution that will meet their needs today and as they grown in the future.

6.2.13 (E) Cloud Security Alliance (8.13)

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 **and** 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)

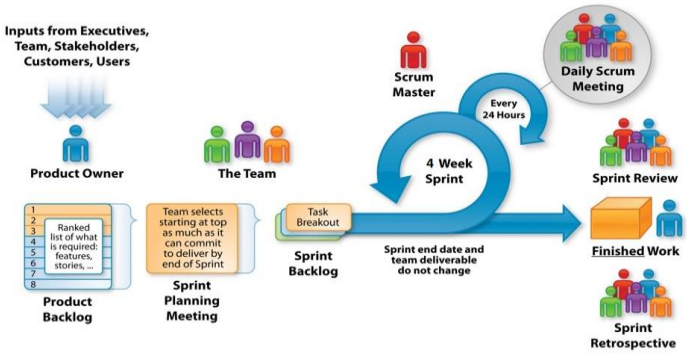
Meridian asserts that their solution is compliant. Please see Document 6 Appendix B, as a separate attachment Exhibit 1 – Consensus Assessments Initiative Questionnaire (CAIQ).

6.2.14 (E) Service Provisioning (8.14)

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

VIP is no stranger to aggressive deadlines and rush implementation requests by purchasing entities. VIP recently delivered two high-profile SaaS regulatory systems, in parallel, for the State of California to meet a legislatively mandated deadline. VIP utilized our Agile Development methodology to increase time to market and deliver the solutions ahead of the mandated date. Our Agile approach allows for an accelerated project ramp up and allows for participating entity collaboration and input early on to deliver at a production-ready solution sooner.

Figure 4 - VIP Agile



VIP's corporate structure and management approach to contracts such as the NASPO Cloud Service Master Agreement allows for immediate responses and expedited project delivery.

In addition, specific to our SaaS offering Meridian LMS, Meridian offers a rapid implementation model for our Multi-tenant SaaS clients. A new site can be stood up with standard configurations and go-live within two (2) to four (4) weeks. If additional items such as HRIS or Historical Data Migration are required, the timeline will extend. For any Emergency fixes, Meridian follows an agile method for product related fixes, therefore, Emergency fixes can typically be applied within one to three business days depending on the nature of the fix.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Meridian's standard implementation is 8-12 weeks. A sample 12-week timeline is outlined below.

- Week 1: Project kickoff
- Weeks 2-5: Discovery Phase: Project planning, client business and functional requirements gathering, and requirements sign-off
- Weeks 6-10: Execution Phase: Design, Configurations, Development, Integrations, Customer Acceptance Testing, and sign-off
- Weeks 11-12: Production environment setup, customer go-live, and project acceptance

6.2.15 (E) Back Up And Disaster Plan (8.15)

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

These accounted for provided they are disclosed. Back up retention policies are flexible to meet client requirements. It is our experience that each client will have different retention and disposition policies so we are flexible to meet a variety of retention needs.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Meridian provides disaster recovery, business continuity, and incident response plans that govern our actions and procedures in the event of an outage, data breach, or natural or man-made disaster. These plans are reviewed and tested annually at minimum to identify and mitigate disaster recovery risks. There are no known current risks awaiting mitigation.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Redundancy is built into our datacenter with redundant power and blended ISPs.

6.2.16 (E) Hosting And Provisioning (8.16)

8.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Provisioning is a standard service for Meridian SaaS clients across a variety of network characteristics (storage, load, etc.). Please see the table below for the Meridian SaaS environment architecture and technology stack.

Environment	Production	Test	All other Environments
Technology Recommendation	5 – KI/KS Servers(4k), 8 VCPU/8GB Ram, Storage (50GB C, 100GB D) +7 – KI/KS Servers (9k), 8 VCPU/8GB Ram, Storage (50GB C, 100GB D) 1 – CS Server (2 VPCU/4GB Ram), or NAS/NetApp Style Storage, Storage (50GB C, 500GB D) 1 - RS Server 8 VCPU/8GB Ram, Storage (50GB C, 100GB D) 1 - Redis/Elastic Server (4 VPCU/8GB Ram), Storage (50GB C, 500GB D) 2 – SQL Servers (Active/Passive Cluster) (16 or 24 CPU/32GB Ram or More) Storage (50GB OS, 1.5TB Data/Logs/Temp/Backup/SQL)	2 – KI/KS Servers, 2 VCPU/4GB Ram, Storage (50GB C, 50GB D) 1 – CS Server (2 VPCU/4GB Ram), or NAS/NetApp Style Storage, Storage (50GB C, 300GB D) 1 - RS Server 2VCPU/2GB Ram, Storage (50GB C, 50GB D) 1 - Redis/Elastic Server (4 VPCU/8GB Ram) Storage (50GB C, 500GB D) 1 – SQL Servers (Active/Passive Cluster) (8 to 16 CPU/32GB Ram) Storage (50GB OS, 500GB Data/Logs/Temp/Backup/SQL)	1 – KI/KS Servers, 2 VCPU/4GB Ram, Storage (50GB C, 50GB D) 1 – CS Server (2 VPCU/4GB Ram), or NAS/NetApp Style Storage, Storage (50GB C, 300GB D) 1 - RS Server 2VCPU/2GB Ram, Storage (50GB C, 50GB D) 1 - Redis/Elastic Server (4 VPCU/8GB Ram) Storage (50GB C, 500GB D) 1 – SQL Servers (Active/Passive Cluster) (8 to 16 CPU/32GB Ram), Storage (50GB OS, 500GB Data/Logs/Temp/Backup/SQL)

8.17.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

VMware is the toolset used for deploying new servers.

2. Creating and storing server images for future multiple deployments

VMware and VM snapshots are used to create and store server images.

3. Securing additional storage space

Meridian provides 1.2 TB of storage (annually, equivalent to 500 MB a month) which far exceeds the storage requirements of most our clients. Additional storage can be purchased in 500 MB blocks if required.

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

Solarwinds provides distinct server level monitoring and Site24x7 provides external monitoring.

6.2.17 (E) Trial and Testing Periods (Pre- and Post- Purchase) (8.17)

8.18.1 Describe your testing and training periods that your offer for your service offerings.

Solution consultants create and manage sandbox environments to allow clients to test the system for a specific period prior to purchase. Once client agrees to become a client, Meridian first provides implementation readiness training to familiarize client stakeholders with the software's features, functions, and configuration options prior to critical functional consulting and system design phases. After the implementation is tailored to client needs, Meridian then provides pre-go-live readiness training to prepare system administrators for a successful go-live. Ongoing training can then be provided (including training for new product releases).

8.18.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Solution consultants create and manage sandbox environments to allow clients to test the system for a specific period prior to purchase. Once the client agrees to purchase Meridian LMS, one of the critical first steps of the implementation is stand-up of the initial test/staging/QA environment.

8.18.3 Offeror must describe what training and support it provides at no additional cost.

Meridian first provides implementation readiness training to familiarize client stakeholders with the software's features, functions, and configuration options prior to critical functional consulting and system design phases. After the implementation is tailored to client needs, Meridian then provides pre-go-live readiness training to prepare system administrators for a successful go-live. Ongoing training can then be provided (including training for new product releases).

6.2.18 (E) Integration and Customization (8.18)

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Meridian LMS supports 2,000+ REST/SOAP APIs exposing the LMS for integration with open-standard third-party technologies, databases, and applications. Webhooks provide a method for

technical users to create and manage integrations without excessive intervention or support from Meridian (we can also build integrations as a service if/where required). Many commonly used tools such as Outlook, WebEx, etc. have pre-built connectors in Meridian LMS negating the need for integration services.

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

VIP has over 22 years' experience tailoring solutions to meet our client's unique needs. When developing a participating addendum, we work closely with the participating entity to define the scope of the unique project and tailor our solution accordingly. In addition, VIP has proposed over 20 value added services that participating entities can utilize to secure the supporting services needed to implement our SaaS offerings. Our proposed SaaS solution, Meridian LMS, is flexible to client needs and can be configured, enhanced, and extended to meet client specifications. For instance, Meridian LMS supports sub-domains. Each domain functions as a standalone version of our product, while maintaining a database backbone with the administrative domain (sub-audiences have a unique system while admins retain centralized control). Each subsequent domain may have its own brand (Logos, fonts, color schemes, etc.) its own custom UX (through our homepage media feeds which are HTML blank-slates), and its own configurations, course catalog, homepage layout, features/modules, etc. Themes may be created using Cascading Style Sheets (CSS) to be applied to core and sub domains as required. Within each domain, there are a plethora of enhancement and configuration options including the ability to disable and hide non-relevant functions. These tools also target audiences outside the traditional four walls of the organization, enabling clients to drive revenue through training by targeting external audiences (customers, members, partners, resellers, etc.) with eCommerce tools while still driving compliance training to their employees. Meridian LMS is highly configurable and extendable at both the organization and audience levels.

6.2.19 8.19 (E) Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

VIP leverages a marketing plan specifically aligned with the NASPO ValuePoint Cloud Solutions Master Agreement. The major elements of the marketing plan include sales enablement and website updates with market-facing content and links to the contract. Upon award, VIP will put out an initial press release, and follow on press releases when participating addendums are executed – primarily via social media sites such as LinkedIn, and Twitter. In addition to updates on our company website specific to NASPO ValuePoint, VIP will also leverage email and phone campaigns to promote the contract to prospects on an ongoing basis. Our sales and marketing team will look for opportunities to tailor specific messaging to the participating entities and in alignment with their unique business needs.

We look forward to collaborating with NASPO ValuePoint to market this contract vehicle to our broad client base.

6.2.20 (E) Related Value-Added Services to Cloud Solutions (8.20)

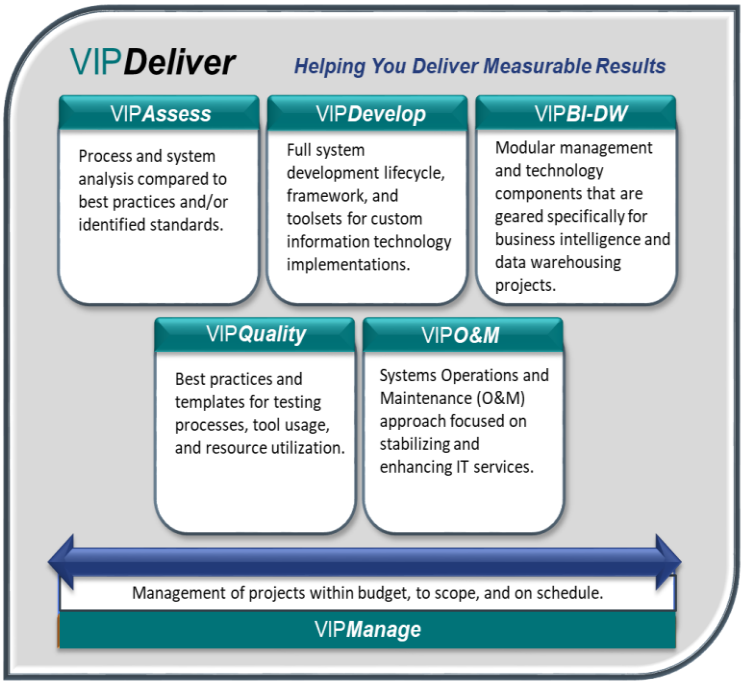
Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

VIP provides value-added services for our SaaS software offering including but not limited to: implementation support, project management, data migration, integration/interface development, change management, risk management, testing/QA, business analysis, hosting, as well as pre-implementation and ongoing training and specialized consulting. We have included over twenty (20) unique roles to provide the Lead State and Participating Entities with a comprehensive menu of value added services which can be tailored for each project.

VIP's value-added services leverage our own time-tested project management methodology called VIPDeliver; a compilation of multiple industry standards and best practices including leveraging:

- Institute of Electrical and Electronic Engineers (IEEE) standards (1012 and 12207) for systems engineering and application development
- Project Management Body of Knowledge (PMBOK®) for project management practices
- International Business Professional Association's Business Analyst's Body of Knowledge (BABOK□)
- Carnegie Mellon University and its Software Engineering Institute

Figure 5: VIPDeliver



The VIPDeliver methodology is based on past experiences and lessons learned from hundreds of projects in the public sector. This methodology includes overarching project management for delivering projects on-time and within budget. It provides guidelines on how to work collaboratively with these entities to identify and mitigate project risks as well as to address issues identified throughout the engagement. VIPDeliver is a proven, robust, yet flexible methodology tailored to government projects to help maximize project success and deliver measurable results.

In addition to the value-added services defined in our proposal, a customer success manager is assigned to each project as an advocate for the client within Meridian and to consult on emerging trends and technologies.

6.2.21 (E) Supporting Infrastructure (8.22)

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

All that is required to use the Meridian LMS SaaS platform is a supported web browser and internet connectivity. We recommend using the latest versions of commonly used web browsers like Safari, Chrome, FireFox, and Internet Explorer.

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Infrastructure costs are borne by Meridian and our hosting partners. This requirement is N/A for browser-based software (client side). Clients will be subscribing to our SaaS model in a managed service hosting environment.

GENERAL TERMS AND CONDITIONS

This Software as a Service Subscription SINGLE Agreement (this "Agreement") is made and entered into as of the effective date set forth below (the "Effective Date") between:

Effective Date of this Agreement: <EFFECTIVE_DATE_MM/DD/YYYY>

MERIDIAN:	CLIENT:
MERIDIAN KNOWLEDGE SOLUTIONS, LLC, a Virginia, limited liability company	<CLIENT_LEGAL_NAME> a <CLIENT_STATE_FULL>, <CLIENT_TYPE_OF_COMPANY>

THESE TERMS AND CONDITIONS CONSTITUTE THE ENTIRE LEGAL AGREEMENT BETWEEN CLIENT AND MERIDIAN KNOWLEDGE SOLUTIONS, LLC ("MERIDIAN") CONCERNING THE ACCESS TO THE PROPRIETARY MERIDIAN LEARNING MANAGEMENT SYSTEM SOFTWARE PROGRAM, ASSOCIATED DOCUMENTATION (hereinafter "Software" and/or "Meridian LMS") AND THE SERVICES PERFORMED BY MERIDIAN IN SUPPORT THEREOF.

A. MERIDIAN has developed certain software programs and associated documentation which MERIDIAN makes available to its CLIENTS ("Subscribers") on a Subscription ("Subscription") basis.

B. CLIENT wishes to use MERIDIAN'S Services and Software in its business operations.

C. MERIDIAN has agreed to provide, and the CLIENT has agreed to pay for and use MERIDIAN'S Services and Software subject to the terms and conditions of this Agreement.

D. In the event there are conflicting terms among the various documents, the order of precedence is as follows: 1) This Agreement; 2) Project Documents; and 3) Exhibit(s).

1. Definitions

a. Authorized User: Employees, agents, and independent contractors of the CLIENT who are authorized to use the Software as described herein.
b. Confidential Information: Information that is proprietary or confidential of MERIDIAN as further defined throughout this Agreement.

c. CLIENT Data: Data that is input by the CLIENT or Authorized Users of the CLIENT into the Software for the purpose of utilizing the Software.
d. Documentation: Documents made available by MERIDIAN to the CLIENT from time to time which may include but is not limited to documents containing Software descriptions, user manuals and other material related to the Software.
e. Effective Date: The day this Agreement takes effect.
f. Initial Subscription Term: The initial term of this Agreement.
g. Internal Business Operations: The internal business processes of an organization. Business operations include the day-to-day activities of the business. Such operations facilitate the achievement of a business' prime function.
h. Standard Business Hours: Monday through Friday 8 am – 8 pm Eastern Standard Time (EST).
i. Services: The access to the software services (Software Services, Implementation Services, collectively, and any Support provided for such Services) provided by MERIDIAN to CLIENT under this Agreement.
j. Software: A single instance of the application provided as a part of the Services Subscription.
k. Subscription Fees: The fees payable to MERIDIAN by the CLIENT for the User Subscriptions.
l. Subscription Term: The term of the Subscription.
m. Support: The general maintenance and technical support Services as set forth herein.
n. Support Policy: MERIDIAN'S policy for providing support in relation to the Services as described herein
o. Service Levels: The Service Level commitments as set forth herein.
p. User Subscription: The subscriptions purchased to grant Authorized Users access to the Services as described herein.
q. Product Extensions: Any modification to the base Meridian LMS application that is specific to the CLIENT's requirements and scope as defined in the Statement of Work and any associated Change Order.
r. Enhancements: Any Meridian governed and deployed product change that increases or modifies the Meridian LMS functionality or feature set; and is not specific to a Client. The release and application of any product Enhancement is at the sole discretion of Meridian.
s. Software Updates: Meridian governed product updates that provide software defect resolutions for existing base Meridian LMS application features or functionality. The updates are provided in patch sets, point releases, or hot/emergency fixes (for example, Version 14.4.1 to 14.4.2). The release and application of any Software Update is at the sole discretion of Meridian.
t. Software Version Upgrades: A major, standalone version of the Meridian LMS application, and is further defined as the CLIENT moving from one major Release of the Meridian LMS application to another (for example, Version 13.0 to 14.0). Software upgrades are not

included in this agreement. The release and application of any Software Version Upgrade is at the sole discretion of Meridian.

2. Subscription

a. Subject to the CLIENT purchasing the User Subscription, the restrictions set forth in this Section and other terms and conditions of this Agreement, MERIDIAN hereby grants to the CLIENT, a non-exclusive, non-transferable right to permit the Authorized Users of the CLIENT to (i) use such Services; and (ii) display such Services solely for the purpose of exercising CLIENT's rights and performing CLIENT's obligations hereunder. The foregoing subscription is subject to the restrictions below and the other terms and conditions of this Agreement. Services shall be used during the Subscription Terms solely for the CLIENT's Internal Business Operations.

b. In relation to the Authorized Users, the CLIENT agrees that:
   i. the maximum number of Authorized Users that it authorizes to access and use the Services shall not exceed the number of User Subscriptions CLIENT has purchased;
   ii. CLIENT will not allow any User Subscription to be used by more than one individual Authorized User during an annual subscription term. A license can be reassigned in its entirety upon the next annual subscription term to another individual Authorized User, in which case the prior Authorized User shall be flagged inactive and no longer have any right to access or use the Services;
   iii. MERIDIAN will monitor the actual number of Authorized Users to ensure compliance with Item (2)(a)(b) above during the annual subscription term.

c. The CLIENT will not intentionally access, store, distribute or transmit any viruses, Trojans or any and all malicious code, or any material during the course of its use of the Services that as outlined below. In the event any of the identified items occur, CLIENT will remove and promptly notify MERIDIAN immediately if there is potential harm to the software.
   i. is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing, racially or ethnically offensive;
   ii. facilitates illegal activity;
   iii. depicts sexually explicit images;
   iv. promotes unlawful violence;
   v. is discriminatory based on race, gender, color, religious belief, sexual orientation, disability, or any other illegal activity;
   vi. causes damage or injury to any person or property; or
   vii. infringes on third party intellectual property, copyright or trademark rights.

MERIDIAN reserves the right, without liability to the CLIENT, to disable the CLIENT's access to any material that breaches the provisions of this clause.

d. The CLIENT shall not except to the extent expressly permitted under this Agreement:
   i. attempt to reproduce, copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute, in whole or in part, any portion of the Software and/or Documentation (as applicable) in any form or media or by any means;
   ii. attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software;
   iii. access all or any part of the Services and/or Documentation in order to build a product or service which competes with the Services, Software and/or the Documentation provided by this Agreement;
   iv. use the Services, and/or Documentation to provide services to third parties; or
   v. subject to the Assignment Section, license, sublicense, sell, rent, lease, transfer, subcontract, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services, and/or Documentation available to any third party except the Authorized Users, or
   vi. attempt to obtain, or assist third parties in obtaining, access to the Services, and/or Documentation, other than as provided under this clause.

e. The CLIENT shall use all reasonable endeavors to prevent any unauthorized access to, or use of, the Services and/or the Documentation and, in the event of any such unauthorized access or use, promptly notify MERIDIAN. The rights provided under this Section are granted to the CLIENT only, and shall not be considered granted to any subsidiary or affiliate of the CLIENT.

f. Additional User Subscriptions.
   vii. The CLIENT may, during any Subscription Term, purchase additional User Subscriptions in excess of the number set out in Schedule 1 and MERIDIAN shall grant access to the Services to such additional Authorized Users in accordance with the provisions of this Agreement.
   viii. If the CLIENT wishes to purchase additional User Subscriptions, the CLIENT shall notify MERIDIAN in writing. MERIDIAN shall evaluate such request for additional User Subscriptions and respond to the CLIENT with approval or disapproval of the request and such approval not to be unreasonably withheld.
   ix. If MERIDIAN approves the CLIENT ’s request to purchase additional User Subscriptions, the CLIENT shall, within thirty (30) calendar days of the date of the MERIDIAN’S invoice, pay MERIDIAN the relevant fees for such additional User Subscriptions as set out in Schedule 1 and, if such additional User Subscriptions are purchased by the CLIENT part way through the Initial Subscription Term or any Renewal Period (as applicable), such fees shall not

be pro-rated for the remainder of the Initial Subscription Term or then current Renewal Period (as applicable).

3. Fees; Payment Terms

a. Fees. In consideration of this Agreement, CLIENT will pay the Subscription fees set forth in Section 27 (the "Subscription Fees"). In consideration of any other products provided or services performed under this Agreement, CLIENT will pay the fees and charges described in Section 27 and the applicable Schedules. On the Effective Date of this Agreement, the Subscription Fees shall be payable with respect to the Initial Subscription Term and at least thirty (30) calendar days prior to each anniversary of the Effective Date, the Subscription Fees shall be payable with respect to the next Renewal Period. If, at any time while using the Services, the CLIENT exceeds the amount of storage space specified in Section 27, MERIDIAN shall charge the CLIENT, and the CLIENT shall pay MERIDIAN'S then current excess data storage fees. MERIDIAN'S excess data storage fees are set out in Section 27 and current as of the Effective Date. MERIDIAN shall be entitled to increase the Subscription Fees, with respect of the additional User Subscriptions purchased, and/or the excess storage fees at the start of each Renewal Period upon thirty (30) calendar days' prior notice to the CLIENT and Section 27 shall be deemed to have been amended accordingly. Fees are non-cancellable and non-refundable except as otherwise stated herein.

b. Payment. All fees and expenses will be due and payable to MERIDIAN within thirty (30) calendar days after the date of invoice. All fees and expenses will be paid to MERDIAN in United States dollars, by wire transfer of funds to an account designated by MERIDIAN or by check sent to MERIDIAN at Attention: Accounts Receivable, Meridian Knowledge Solutions, LLC, 80 Iron Point Circle, Suite 100, Folsom, CA 95630 unless otherwise specified by MERIDIAN. All past-due payments will bear interest at the rate of one and one-half percent (1½%) per month or the maximum rate allowed by law, whichever is less. MERIDIAN shall have the right to terminate the Agreement for default/cause if the CLIENT does not pay MERIDIAN'S undisputed invoices within the terms contained herein. All outstanding invoices will be due and payable immediately upon such termination. If CLIENT does not pay MERIDIAN for any undisputed outstanding invoices, and MERIDIAN incurs any additional costs including, but not limited to court costs, attorney's fees and other damages, in the collection of said invoices, MERIDIAN shall have the right to recover the additional costs from CLIENT.

c. Taxes. CLIENT acknowledges and agrees that it is responsible for the payment of all applicable taxes and duties, including, without limitation, sales, use, excise, value added and franchise taxes, associated with this Agreement, the products provided and the services performed under this Agreement, except for taxes based on MERIDIAN'S income.

d. The CLIENT shall on the Effective Date provide to MERIDIAN valid, up-to-date and complete approved purchase order information acceptable to MERIDIAN and any other relevant information needed by MERIDIAN to invoice CLIENT.

e. If MERIDIAN has not received payment within thirty (30) calendar days after the due date of any undisputed invoice, and without prejudice to any other rights and remedies of MERIDIAN, MERIDIAN may, without further liability to the CLIENT, disable the CLIENT's passwords, accounts and access to all or part of the Services. MERIDIAN shall be under no further obligation to provide any or all of the Services while the invoice(s) concerned remain unpaid; and MERIDIAN shall have the right to terminate the Agreement for default if the CLIENT does not pay MERIDIAN'S undisputed invoices within the terms contained herein. All outstanding invoices will be due and payable immediately upon such termination. If CLIENT does not pay MERIDIAN for any undisputed outstanding invoices, and MERIDIAN incurs any additional costs including, but not limited to court costs, attorney's fees and other damages, in the collection of said invoices, MERIDIAN shall have the right to recover the additional costs from CLIENT.

f. PCI Compliance. In the event CLIENT engages in payment card transactions as part of the services provided to MERIDIAN, CLIENT shall comply with the Payment Card Industry Data Security Standard ("CI-DSS") and any amendments or restatements of the PDI DSS during the Term of this agreement. CLIENT accepts responsibility for the security of customer credit card data in its possession, even if all or a portion of the services to MERICAN are subcontracted to third parties.

4. Proprietary Rights

a. CLIENT acknowledges and agrees that the Software is protected by U.S. and international copyright, patent, trademark, trade secret and other intellectual property rights and registrations. CLIENT acknowledges that all right, title and interest in and to the Software and all intellectual property rights thereto will be owned solely by MERIDIAN and its licensors, as applicable. CLIENT will not remove, obliterate, obscure or alter any copyright or other proprietary rights notice that appears on the Software. Except for the limited rights expressly granted to CLIENT under this Agreement, CLIENT is not granted any other rights in or to the Software. All rights in and to the Software not specifically granted herein are reserved to MERIDIAN and its licensors, as applicable.

5. Confidentiality Obligations

a. Confidential Information. "Confidential Information" means any and all information that is of a confidential, proprietary or trade secret nature that is furnished or disclosed by MERIDIAN to CLIENT under this Agreement. Without limiting the generality of the foregoing, "Confidential Information" includes the Software (including the object code and

source code forms thereof), the specific business terms of this Agreement and any other information that is marked as "Confidential," "Proprietary," "Trade Secret" or in some other manner to indicate its confidential, proprietary or trade secret nature. “Confidential Information” will not include: (i) information that is or becomes publicly known through no fault of CLIENT; (ii) information received from a third party that was disclosed without breach of any confidentiality obligation; (iii) information approved for release by written authorization of Meridian; (iv) information developed or created independently by CLIENT without reference to, or use of, MERIDIAN’S Confidential Information; or (v) information that may be required by law, regulation or an order of any court, agency or proceeding to be disclosed, provided that CLIENT will provide MERIDIAN with written notice of any such required disclosure once CLIENT has knowledge of it and will help MERIDIAN at the expense of CLIENT to the extent reasonable to obtain an appropriate protective order.

b. Non-Disclosure. All Confidential Information will remain the property of MERIDIAN and CLIENT will not be deemed by virtue of its access to MERIDIAN’S Confidential Information to have acquired any right or interest in or to any such Confidential Information, other than as specifically set forth herein. CLIENT agrees: (i) to hold the Confidential Information in strict confidence; (ii) except as expressly authorized in this Agreement, not to disclose any Confidential Information to any third party other than employees and independent contractors of CLIENT who have a need to know the Confidential Information for the purposes of this Agreement and who are subject to a confidentiality agreement that affords at least as much protection to the Confidential Information as this Section 6; (iii) to use the Confidential Information solely and exclusively in accordance with the terms of this Agreement in order to carry out CLIENT ’s obligations and exercise its rights under this Agreement; and (iv) to notify MERIDIAN promptly of any unauthorized use or disclosure of the Confidential Information and to cooperate with and assist MERIDIAN in every reasonable way to stop or minimize such unauthorized use or disclosure.

c. Injunction. CLIENT agrees that if a court of competent jurisdiction determines that CLIENT has breached, or attempted or threatened to breach, its confidentiality obligations to MERIDIAN or MERIDIAN’S proprietary rights, MERIDIAN will be entitled to obtain appropriate injunctive relief and other measures restraining further attempted or

threatened breaches of such obligations. Such injunctive relief or other measures will be in addition to, and not in lieu of, any other rights and remedies available to MERIDIAN.

6. CLIENT Data

a. The CLIENT shall own all rights, title and interest in and to all of the CLIENT Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the CLIENT Data.

b. MERIDIAN shall follow its commercially reasonable backup procedures for CLIENT Data and said procedure may be amended by MERIDIAN in its sole discretion from time to time based upon best practices. In the event of any loss or damage to CLIENT Data, the CLIENT's sole and exclusive remedy shall be for MERIDIAN to use reasonable commercial activities to restore the lost or damaged CLIENT Data from the latest back-up of such CLIENT Data maintained by MERIDIAN in accordance with the backup procedure described herein. MERIDIAN shall not be responsible for any loss, destruction, alteration or disclosure of CLIENT Data caused by any third party (except those third parties subcontracted by MERIDIAN to perform services related to CLIENT Data maintenance and back-up).

c. MERIDIAN shall, in providing access to the Services, comply with its Privacy Policy relating to the privacy and security of the CLIENT Data available at http://www.meridianks.com/privacy-statement/ or such other Policy as may be given to the CLIENT from time to time, as such document may be amended from time to time by MERIDIAN in its sole discretion.

d. MERIDIAN strongly recommends that CLIENT not store or process Personally Identifiable Information (PII) or Personally Identifiable Health Information (PHI) within the Software. PII is defined as information that can be used to uniquely identify a single individual and may include an individual’s name in combination with a Driver’s License, Social Security Number or Credit Card Information. The definition of PII varies depending on international, federal, state and local laws and the definition contained herein shall be used for reference purposes only and shall not be construed as covering all possible definitions of PII. PHI is defined as any information that is related to an individual’s health record as defined by the Health Insurance Portability and Accountability Act (HIPAA).

e. PHI/PII Processing - The parties shall comply, and warrant that they have complied, with implementing all applicable data protection and privacy laws and regulations in any relevant jurisdiction (together, the “Data Protection Laws”); and where, in connection with this Agreement, the Software is processing information related to PHI/PII on behalf of the CLIENT, MERIDIAN shall:

i. Process the PHI/PII only on the written instructions of CLIENT;

ii. Make all reasonable efforts to implement appropriate technical and organizational measures to protect those PHI/PII against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

iii. Return or destroy all such personal data promptly upon the termination of this Agreement, or at any time during the term of this Agreement upon written instructions from CLIENT;

iv. Not disclose PHI/PII to any person except as required or permitted by this Agreement or with CLIENT's written consent;

v. Provide full cooperation and assistance to CLIENT in implementing any procedures required in order to comply with data privacy laws to which CLIENT is subject, as advised by CLIENT from time to time;

vi. Not process PHI/PII except to the extent reasonably necessary to the performance of this Agreement;

vii. Notify CLIENT immediately in the event of any breach of the security of such personal data, and cooperate with CLIENT in any post- breach investigation or remediation efforts; and

viii. Notify CLIENT promptly in the event that MERIDIAN is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any PHI/PII to any person other than CLIENT.

The CLIENT shall make all reasonable efforts to ensure that those Personal Data are accurate and up to date at all times, to the extent that it is within CLIENT's ability to do so.

The Parties hereto agree, that the above warranties relating to PHI and PII are Meridian's sole responsibilities related to the processing and control of CLIENT PHI and PII.

7. European Union Clients

In the event that CLIENT will access PII originating from a country in the European Economic Area ("EEA") or from a country outside the EEA, MERIDIAN shall, if requested by CLIENT, will comply with the applicable Privacy Law Legislation in coordination with the European Commission, relating to requirements of the European Union's Directive on Data Protection. CLIENT warrants that it has the consent of its employees, independent contractors or any other individual whose PII is being processed and/or transmitted within the Services and MERIDIAN shall have no liability should CLIENT not have received such consent. CLIENT will indemnify, defend and hold MERIDIAN harmless should any such individual or group of individuals bring any suit against MERIDIAN for violation of any applicable law.

8. Limited Warranty / Acceptance

a. Meridian warrants that it will perform the Services in a manner consistent with industry standards reasonably applicable to the performance thereof. MERIDIAN does not warrant that CLIENT's use of the Services will be uninterrupted or error free. The limited warranties set forth in this Agreement do not apply to any deviation by the Software from the specifications set forth in the applicable Schedule that is caused by, or results from, (i) modification of the software (ii) improper usage of Software API's (Application Programming Interfaces) or the introduction/import of corrupt data into the Software by anyone other than Meridian; (iii) use of the Services for any purpose other than that authorized in this Agreement; (iv) use of the Services in combination with other software, data or products that are defective or incompatible with, or are not authorized by MERIDIAN for use with, the Services; (v) any malfunction of CLIENT 's software, hardware, computers or computer-related equipment; (v) CLIENT'S failure to use any Updates made available by Meridian; or (vi) an event of Force Majeure (defined below).

b. MERIDIAN DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM THE SOFTWARE AND OTHER PORTIONS OF THE INTERNET. SUCH FLOW DEPENDS IN LARGE PART ON THE PERFORMANCE OF INTERNET SERVICES PROVIDED OR CONTROLLED BY THIRD PARTIES. AT TIMES, ACTIONS OR INACTIONS OF SUCH THIRD PARTIES CAN IMPAIR OR DISRUPT CUSTOMER'S CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF). ALTHOUGH MERIDIAN WILL USE COMMERCIALLY REASONABLE EFFORTS TO TAKE ALL ACTIONS IT DEEMS APPROPRIATE TO REMEDY AND AVOID SUCH EVENTS, MERIDIAN CANNOT GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR. ACCORDINGLY, MERIDIAN DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO SUCH EVENTS.THE FOREGOING WARRANTIES ARE MADE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR COURSE OF PERFORMANCE. EXCEPT AS EXPRESSLY PROVIDED HEREIN, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH CLIENT'S ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT, THE SERVICES ARE PROVIDED "AS IS," AND MERIDIAN DISCLAIMS ANY WARRANTY AS TO THE QUALITY, OPERATION OF, ACCESS TO OR USE OF ALL OR ANY PART OF THE SOFTWARE AND ANY WARRANTY THAT (I) THE SERVICES WILL OPERATE UNINTERRUPTED OR ERROR-FREE, (II) THE RESULTS ARISING OUT OF THE USE OF THE SERVICES WILL BE ACCURATE, COMPLETE OR ERROR-FREE, OR (III) THE

SERVICES WILL MEET THE NEEDS OF CLIENT OR ITS CLIENTS, AGENTS OR SUPPLIERS.

c. Acceptance of the Software will be upon the CLIENT's receipt of the URL from MERIDIAN, where CLIENT will be provided access to the Software.

9. Other CLIENT Obligations

a. The CLIENT shall provide MERIDIAN with:
   i. all necessary cooperation in relation to this Agreement;
   ii. all necessary access to such information as may be required by MERIDIAN in order to render the Services, including but not limited to CLIENT Data, security access information and configuration services;
   iii. comply with all applicable laws and regulations with respect to its activities under this Agreement;
   iv. carry out all other CLIENT responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the CLIENT's provision of such assistance as agreed by the parties, MERIDIAN may adjust any agreed timetable or delivery schedule as reasonably necessary;
   v. ensure that the Authorized Users use the Services and the Documentation in accordance with the terms and conditions of this Agreement and shall be responsible for any Authorized User's breach of this Agreement;
   vi. obtain and maintain all necessary licenses, consents, and permissions necessary for MERIDIAN, its employees, subcontractors and/or agents to perform their obligations under this Agreement, including without limitation the Services;
   vii. ensure that its network and systems comply with the relevant specifications provided by MERIDIAN from time to time; and
   viii. be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to MERIDIAN'S data centers, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the CLIENT's network connections or telecommunications links or caused by the internet.

10. Indemnification

a. MERIDIAN and CLIENT agree to indemnify, defend and hold harmless the other, and their respective officers, directors, employees, partners and shareholders, from and against all claims, losses, demands, damages or costs, including attorneys' fees, arising from any source, including but not limited to the intentional or negligent acts, errors or omissions of the other or its officers, directors, employees, partners, and shareholders, or anyone for whom either MERIDIAN or CLIENT is legally liable, arising out of the performance of this Agreement. MERIDIAN will have no obligation to defend CLIENT with

respect to any claim, demand, action or proceeding, described herein, that is based upon (i) use of other than the then-current release of the Software, if infringement could have been avoided by use of the then-current release and the then-current release has been made available to CLIENT; (ii) use of the Services in conjunction with CLIENT's data, where use with such data gave rise to the infringement claim; (iii) use of the Services with other software, where use of such other software gave rise to the infringement claim; (iv) use of any Services in a manner inconsistent with its documentation; or (v) use of any Services in a manner that breaches this Agreement. CLIENT will defend MERIDIAN from and against any and all liability, damage, loss or expense (including reasonable attorneys' fees) arising out of any claim, demand, action or proceeding based on allegations arising as a result of (i) use of the Services by CLIENT in conjunction with any data, equipment or software not provided by MERIDIAN, where the Services would not itself be infringing or otherwise the subject of the claim; (ii) use of the Services by CLIENT in a manner not permitted by this Agreement; (iii; (iv) use of the Services by CLIENT in any unlawful, improper or inappropriate manner or for any unlawful, improper or inappropriate purpose; (v) any claim of infringement of any patent or copyright or misappropriation of any trade secret in which CLIENT or any affiliate of CLIENT has a pecuniary or other material interest; or (vi) breach of any of CLIENT's warranties or covenants.

11. Term and Termination

a. The term of this Agreement will begin on the Effective Date and shall continue for the Initial Subscription Term and, thereafter, shall be automatically renewed for successive periods of twelve (12) months ("Renewal Period"), unless:
    i. Either party notifies the other party of termination, in writing, at least sixty (60) calendar days before the end of the Initial Subscription Term or any subsequent Renewal Period, in which case this Agreement shall terminate upon the expiration of the applicable Initial Subscription Term or Renewal Period; or
    ii. Otherwise terminated in accordance with the provisions of this Agreement; and the Initial Subscription Term together with any subsequent Renewal Periods shall constitute the entire Subscription Term.

b. Either party may terminate this Agreement immediately upon notice to the other party if such other party materially breaches a provision of this Agreement or Schedule, as applicable, and fails to cure such breach within thirty (30) calendar days after receipt of notice of such breach from the non-breaching party. If, in the sole judgment of the non-breaching party, such breach cannot reasonably be cured within such thirty (30) calendar day period, the non-breaching party may, in its sole discretion, grant the breaching party an additional thirty (30) calendar day period following the expiration of the first thirty (30) calendar day period in which to cure such breach; provided that the non-breaching party may terminate this Agreement or such Schedule, as applicable, immediately if the

breaching party has failed to cure such breach within such second thirty (30) calendar day period.

c. Either party may terminate this Agreement immediately upon notice to the other party if such other party (i) files for or has filed against it a bankruptcy petition and such petition is not dismissed within sixty (60) calendar days after the filing date, (ii) becomes insolvent or (iii) makes an assignment for the benefit of its creditors.

12. Term and Termination

a. Upon the expiration or termination of this Agreement,
   i. all rights granted to CLIENT under this Agreement will immediately terminate;
   ii. CLIENT will cease any further use of the Services.

b. At MERIDIAN'S request, CLIENT will verify in writing to MERIDIAN that CLIENT has taken the actions described in clauses Section 12(a)(ii). MERIDIAN may destroy or otherwise dispose of any of the CLIENT Data in its possession unless MERIDIAN receives, no later than ten (10) business days after the effective date of the termination of this Agreement, a written request for the delivery to the CLIENT of the then most recent back-up of the CLIENT Data. MERIDIAN shall use reasonable commercial efforts to deliver the back-up to the CLIENT within thirty (30) calendar days of its receipt of such a written request, provided that the CLIENT has, at that time, paid all fees and charges outstanding at and resulting from termination (whether or not due at the date of termination). The CLIENT shall pay all reasonable expenses incurred by MERIDIAN in returning or disposing of CLIENT Data. The accrued rights of the parties at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination shall not be affected or prejudiced. The rights and obligations of each of the parties set forth in Sections 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14, 17, 18, 20, 21, 23, 24 and 25 and any other Section or Statement herein that by its nature is intended to survive will survive the expiration or termination of this Agreement. Any payments owed by CLIENT as of the date of expiration or termination of this Agreement will be made by CLIENT without any holdback, setoff, delay or suspension.

13. Limitation of Liability

a. EXCEPT IN THE CASE OF AN INFRINGEMENT BY CLIENT OF ANY OF MERIDIAN'S PROPRIETARY RIGHTS, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY LOST PROFITS, LOST DATA OR SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY NATURE, FOR ANY REASON, INCLUDING, WITHOUT LIMITATION, THE BREACH OF THIS AGREEMENT OR ANY TERMINATION OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY) OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN WARNED OF THE

POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OF ANY KIND. EXCEPT AS EXPRESSLY SET FORTH HEREIN, ALL REMEDIES, INCLUDING, WITHOUT LIMITATION, THE TERMINATION OF THIS AGREEMENT AND ALL OF THE REMEDIES PROVIDED BY LAW (AND NOT EXCLUDED PURSUANT TO THE FOREGOING SENTENCE) WILL BE DEEMED CUMULATIVE AND NOT EXCLUSIVE. IN NO EVENT WILL THE LIABILITY OF MERIDIAN UNDER THIS AGREEMENT EXCEED THE TOTAL FEES PAID BY CLIENT HEREUNDER DURING THE TWELVE (12) MONTHS PRIOR TO THE DATE ANY CLAIM IS MADE AGAINST MERIDIAN.

14. Government Use/Procurement

a. Meridian provides the Service and access to the Software for ultimate U.S. Government end use solely in accordance with the following: Government technical data and software rights related to the Service and the Software include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not conveyed under these terms, it must negotiate with Meridian to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

b. Each party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Service and the Software. Without limiting the foregoing: (a) each party represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports; and (b) each Party shall not permit any User to access or use the Service and the Software in violation of any U.S. export embargo, prohibition or restriction.

15. Assignment

a. CLIENT may not assign or otherwise transfer this Agreement or its rights and obligations hereunder without the prior written consent of MERIDIAN, which consent will not be unreasonably withheld. Any transaction or series of transactions in which (i) more than fifty percent (50%) of the outstanding voting stock or membership interests of CLIENT are transferred to a third party, or (ii) all or substantially all of CLIENT's assets are sold to a third party, will be deemed an assignment of this Agreement. Any purported assignment or other transfer without the consent of MERIDIAN (a) will be void and of no force or effect, and (b) will constitute a material breach of this Agreement.

16. Force Majeure

a. Except for a party's payment obligations hereunder, neither party will be deemed in default of this Agreement to the extent that performance of its obligations, or attempts to cure any breach thereof, are delayed or prevented by reason of any act of God, fire, natural disaster, accident, terrorist attack, act of government, network or telecommunication system failure, sabotage or any other cause beyond the control of such party ("Force Majeure"), provided that such party promptly gives the other party notice thereof. In the event of such Force Majeure, the time for performance or cure will be extended for a period equal to the duration of the Force Majeure but not in excess of six (6) months.

17. Severability

a. If a court of competent jurisdiction determines that any provision of this Agreement is illegal, invalid or otherwise unenforceable for any reason, such provision will be deemed stricken to the extent that it is illegal, invalid or otherwise unenforceable. All remaining provisions will remain in full force and effect and this Agreement will be interpreted as if it had not contained the severed provision.

18. Governing Law

a. Issues regarding the validity, ownership or enforcement of any copyright, patent, trademark or other proprietary right licensed or sublicensed hereunder will be determined under the applicable law of the United States and the Commonwealth of Virginia, as applicable. With respect to all other issues, this Agreement will be construed under and governed by the substantive laws of the Commonwealth of Virginia without resort to conflict of laws principles. Each party agrees that any legal proceeding commenced by one party against the other party under this Agreement will be brought in any state or Federal court having jurisdiction over Fairfax County, Virginia. Each party submits to such jurisdiction and waives any objection to venue or claim of inconvenient forum. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

19. Headings

a. Captions and section headings used herein are for reference purposes only and will not control or alter the meaning of this Agreement as set forth in the text.

20. Waiver

a. A waiver of any right under this Agreement is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

b. Unless specifically provided otherwise, rights arising under this agreement are cumulative and do not exclude rights provided by law.

21. Notices

a. Any notice required to be given under this agreement shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other party at its address set out in this agreement, or such other address as may have been notified by that party for such purposes. A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 AM on the first business day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post.

If to MERIDIAN:
Attention: Contracts
Meridian Knowledge Solutions, LLC
2001 Edmund Halley Drive, Suite 400
Reston, VA 20191
With a copy to:
Attention: Legal Department
Meridian Knowledge Solutions, LLC
80 Iron Point Circle, Suite 100
Folsom, CA 95630

If to CLIENT:
Attention: <CLIENT_ATTENTION_LEGAL>
<CLIENT_LEGAL_ADDRESS_1>
<CLIENT_LEGAL_ADDRESS_2>
<CLIENT_LEGAL_CITY_STATE_ZIP>
<CLIENT_LEGAL_NAME>

22. No Partnership or Joint Venture.

a. Nothing in this Agreement is intended to or shall operate to create a partnership between the parties, or authorize either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power). This Agreement shall not prevent MERIDIAN from entering into similar agreements with third

parties, or from independently developing, using, selling or licensing documentation, products and/or services which are similar to those provided under this Agreement.

23. Non-Solicitation.

a. In addition to the obligations set forth in Section 5, during the term of this Agreement and for a period of twelve (12) months immediately following the last occurrence of any introductions, interviews, or provision of services under this Agreement, CLIENT agrees not to solicit or hire, indirectly or directly, in either an employee or independent contractor capacity, any individual who (i) was introduced under this Agreement; (ii) the CLIENT has interviewed under this Agreement; (iii) has provided services under this Agreement, or (iv) the CLIENT or its employees, representatives and or agents have received information about or as the result of any introduction, interview or service provided under this Agreement. Should the CLIENT breach this Section 23 of the Agreement in any instance the CLIENT will pay MERIDIAN an amount of two (2) times the then current annual salary (including any applicable bonus compensation) of the individual solicited directly to MERIDIAN. Said payment will be made within fifteen (15) calendar days of the breach as notified in writing by MERIDIAN to the CLIENT. The Parties hereto further agree that the limit on liability as defined herein does not apply to this Section 23.

24. Disputes and Arbitration.

a. The parties agree that in the event of a dispute or alleged breach they will work together in good faith to resolve the matter internally by escalating it to higher levels of management and, if necessary, to use a mutually agreed upon alternative dispute resolution mechanism (other than arbitration) prior to resorting to arbitration. If the parties are unsuccessful at resolving said dispute or alleged breach, then the parties shall seek arbitration. Except as set forth in Section 5, the parties agree to submit to binding arbitration within six (6) months of the last event giving rise to any controversy arising out of this Agreement or involving the construction or application of any of the terms of this Agreement and to waive any statute of limitations to the contrary. Notification to the other party of a written request for arbitration shall comply with Section 21 governing Notices. Any timely and properly noticed request for arbitration shall be submitted to binding arbitration through the American Arbitration Association pursuant to its Commercial Arbitration Rules. Each party shall pay for its own attorneys' fees and costs for the arbitration. The parties shall split equally the cost of the arbitrator. Both parties are entitled to conduct discovery in accordance with any applicable law. The arbitrator shall apply Virginia and Federal law to the issues presented and shall issue a written memorandum of decision. The decision of the arbitrator shall be final and binding, and the parties waive the right to a jury trial, a trial de novo or appeal except for the purpose of enforcing the arbitrator's decision. The prevailing party will be entitled to recover reasonable attorneys' fees and costs of any action for enforcement, the amount of any such attorneys' fees and costs award to be determined by the Arbitrator.

b. Except as set forth in Section 5 with regard to injunctive relief, the parties expressly state that it is their intent to arbitrate disputes between them. Therefore, this Agreement shall be construed so as to be consistent with applicable Federal and Virginia law and to be enforceable to the maximum extent allowable by law to provide arbitration as the forum to resolve their disputes. If necessary, any portion of this Agreement that is unenforceable by law shall be stricken, and the arbitrator or the court, as the case may be, shall have the power to reform this Agreement to the extent necessary to comply with applicable law and to give effect to the parties' intent that they shall arbitrate their disputes.

25. Publicity

CLIENT grants MERIDIAN permission to utilize the CLIENT's trademarks, trade names, or other designations in any promotion, press release or publication.

26. Entire Agreement

a. Except as otherwise provided for herein, this Agreement constitutes the entire agreement between the parties pertaining to the subject matter hereof and supersedes all prior and contemporaneous agreements, negotiations and understandings, oral or written, between the parties with respect to the subject matter hereof. This Agreement will be binding on and inure to the benefit of the legal representatives, successors and permitted assigns of the parties. This Agreement may not be modified or refined unless amended by both Parties under a written and signed amendment. The issuance of any additional terms and conditions by either Party hereto included with purchase orders or other documents are null and void. In the event of any conflict between these General Terms and Conditions and a provision of any Schedule, the provision of the Schedule will control, but only with respect to the subject matter of the Schedule.

27. Subscription Term and Fees

a. Software: Meridian LMS

b. Modules/Components. The following additional modules and components are included/enabled:

i. None

c. Languages. The following language packs are included/enabled:

ii. English (US) [included]

d. Initial Subscription Term

e. The initial term of this subscription will be <SUBSCRIPTION_TERM> commencing from the Effective Date of this Agreement.

f. Renewal Period Terms
Upon expiration of the Initial Subscription Term, this Agreement will be renewable in subsequent <SUBSCRIPTION_RENEWAL_TERM> terms based on the then current pricing for the Applications, Modules/Components, and Languages listed above.

g. Number of Authorized Users. Maximum of <AUTHORIZE_USERS_> active users
"Authorized Users" is defined as the total number of user accounts that have access to the system during the annual subscription term.

h. Additional User Subscription Fees
Additional "Authorized Users" can be added at any time during the Initial Term or Renewal Period Terms based on the then current Subscription pricing for additional users

i. Bandwidth and Storage
The following bandwidth and storage limitations are included as part of this Agreement. Any additional bandwidth or storage required by CLIENT will be subject to current published price list.

- Bandwidth: 100GB/month (1.2 TB/annually – measured annually)
- Additional content storage is priced at $500 annually for 100 GB.

Bandwidth will be measured based upon total in/out traffic. Bandwidth will be monitored on a monthly basis in relation to the commitments levels, however bandwidth will be measured based upon total usage over the annual term. Overage fees may apply go consuming more bandwidth.

a. Subscription Fees
The following subscription fees apply to this Agreement: **<SUBSCRIPTION_FEES>** per year during the Initial Subscription Term.

b. Set-up Fee
The following set up fees apply to this Agreement, and are defined in Schedule One (1) of this agreement**: <SETUP_FEES>**

c. Optional Services/Module Fees
The following optional modules and services are available. The respective fees are included in Schedule One (1) of this agreement.
OPTIONAL_MODULES_SERVICE_FEES>

d. Optional Historical Data Migration
The respective scope of Services to be provided are defined in Schedule One (1) of this agreement **<OPTIONAL_DATA MIGRATION_SERVICE_FEES>**

28. Service Level Agreements: **Software Support, Software Availability and Maintenance**
The Services provided by MERIDIAN under this agreement are bound by the Service Level Agreement (SLA) as described herein. In the case of an SLA violation, the respective remedies described herein will apply. The SLA penalty applicable in any given month is subject to a total cumulative penalty cap of ten percent (10%) of the current month's hosting service fees ("Service Credits"). Any Service Credits due under this agreement will be credited promptly but in no event later than the quarter following the calculation of the Service Credit.
MERIDIAN will be provided a ramp up period of ninety (90) days from software Go Live (Production go live date) before any SLA requirements and subsequent remedies go into effect.

a. System Availability: will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time (measured in minutes) during such month, and thereafter dividing the difference so obtained by the total time during such month. Represented algebraically, System Availability for any particular calendar month is determined as follows:

$$\text{System Availability} = \frac{(\text{Total Monthly Time} - \text{Unscheduled Downtime})}{\text{Total Monthly Time}}$$

Note: "Total Monthly Time" is deemed to include all minutes in the relevant calendar month excluding minutes of downtime caused by Scheduled Downtime, only to the extent such minutes are included within the Subscription Agreement Term.

MERIDIAN will undertake commercially reasonable measures to ensure that System Availability equals or exceeds 99.70 % during each calendar month.

a. **Measurement and Reports:** MERIDIAN will monitor System Availability metrics on an ongoing basis. All measurements of System Availability will be calculated on a monthly basis for each calendar month during the term of this agreement. MERIDIAN shall provide the System Availability report to CLIENT, on an as required basis, when requested by CLIENT. This report will contain performance metrics against the System Availability SLA obligations as depicted herein; and specific to unscheduled downtime events only.

b. **Remedies:** In the event System Availability is not equal to or greater than 99.70% for a given month, CLIENT will be entitled to service level credits against its subsequent payment obligations (as set forth in this Subscription Agreement) according to the following:

System Availability	Available Credit *(% of monthly service fee)*
99.70% - 100.00%	No Credit.
95.00% - 99.69%	Three percent (3%) of the applicable monthly hosted service fees for the applicable calendar month.
90.00% - 94.99%	Six percent (6%) of the applicable monthly hosted service fees for the applicable calendar month.
<89.99%	Ten percent (10%) of the applicable monthly hosted service fees for the applicable calendar month.

CLIENT's credits under this section are CLIENT's sole and exclusive remedy with respect to any Unscheduled Downtime or any failure by MERIDIAN to meet the Service Availability required by this agreement. The monthly available credit is capped at the lesser of $5,000 or the total cap as set forth in the System Availability section herein.

MERIDIAN will exercise commercially reasonable efforts to initiate remedial activity within two (2) hours of CLIENT reporting the unscheduled downtime to MERIDIAN.

c. **Exceptions.** CLIENT shall not receive any credits in connection with any failure or deficiency Availability caused by or associated with:

iii. Force Majeure events beyond MERIDIAN's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, ecommerce software, payment

gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this Schedule;

iv. Failure of access circuits to the ISP Network, unless such failure is caused solely by MERIDIAN;

v. Scheduled maintenance and emergency maintenance and upgrades;

vi. DNS issues outside the direct control of MERIDIAN;

vii. Issues with FTP, POP, or SMTP CLIENT access;

viii. False Schedule breaches reported as a result of outages or errors of any MERIDIAN measurement system;

ix. CLIENT's acts or omissions (or acts or omissions of others engaged or authorized by CLIENT), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP), any negligence, willful misconduct, or use of the Services in breach of MERIDIAN's Terms and Conditions and Acceptable Use Policy;

x. E-mail or webmail delivery and transmission;

xi. DNS (Domain Name Server) Propagation; and / or

xii. Outages elsewhere on the Internet that hinder access to your account. MERIDIAN is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. MERIDIAN will guarantee only those areas considered under the control of MERIDIAN: MERIDIAN server links to the Internet, MERIDIAN'S routers, and MERIDIAN'S servers.

d. Software Support

MERIDIAN will provide up to two (2) apply service packs per Subscription term year. This includes, but is not limited to the following: product improvements, and enhancements as they are released. "Support" is provided by the MERIDIAN Client Care Center (CCC), and includes the following:

- Administrator help desk support to provide guidance on the use of existing product functions for up to five (5) named system administrators.
- Troubleshooting of reported functional issues including assistance with the following types of questions or issues:
  i. Investigating and finding the cause of issues associated with software functions. MERIDIAN will determine whether the issue is inherent in the base product, or the result of integrations done specifically for CLIENT.
  ii. For base product issues, the CCC will report all issues and desired modifications to the MERIDIAN product team. All product issues will be reported, tracked and managed by the CCC in coordination with the MERIDIAN product team. Determination of the need and prioritization of Updates to address reported issues is at the sole discretion of MERIDIAN.

Support will be provided during Standard Business Hours, Monday-Friday from 8am to 8pm Eastern Time by telephone and/or support ticket via online Support portal.

The Client acknowledges from time to time in Company's sole discretion but using commercially reasonable efforts to minimize any disruption of the Service, MERIDIAN will schedule standard system maintenance, including service pack updates to the Software and/or system, in which case MERIDIAN will announce the scheduled maintenance via e-mail to CLIENT's designated e-mail address.

e. Software Support Severity Level Definitions

All reported issues to the CCC will be assigned a Severity Level which defines the critical nature of the problem. The Severity Level will drive CCC response to the CLIENT, internal escalation process, on procedures per a defined timeline.

The following table defines the four standard Severity Levels that will be assigned to MERIDIAN documented issues. Subsequent tables outline the notification and escalation processes for each defined Severity Level.

Severity Level	Severity Description	Response Time
1 Critical	Issue that causes complete loss of service to the CLIENT's production environment and work cannot reasonably continue. Workarounds to provide the same functionality are not possible and cannot be found in time to minimize the impact on the CLIENT's business. The problem has one or more of the following characteristics: Fifty percent of users cannot access the system. Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, loss of functionality that is financially impacting. Severe performance degradation rendering the system unusable. Loss of data that cannot be reasonably retrieved. Security vulnerabilities that could expose PII data.	One (1) Hour

2 Major	Issue where operation of the system is considered severely limited, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics: A software error for which there is a Customer acceptable workaround. Self-contained issue that does not impact the overall functionality of the software. Minimal performance degradation which impacts productivity.	One (1) business day
3 Minor	Issue that causes no loss of service and in no way impedes use of the system. The problem has one or more of the following characteristics: Guidance on the use of existing base product functions and Customer accepted modifications. Cosmetic issue such as misspelled words or misaligned text. Enhancement requests to update functionality.	Two (2) business days
4 Minimal	Questions regarding system functionality where product user guides are confusing or non- existent and answers are limited to under thirty (30) minutes.	Three (3) business days

CLIENT Responsibilities: To provide effective support, additional information may be required by CLIENT. Additional details regarding MERIDIAN and CLIENT responsibilities are documented in the MERIDIAN Customer Support Policy.

f. Support Exclusions.
The following services are not included Support, but can be provided as separate, optional tasks:

i. Training on Software functions and modifications in excess of standard help desk support. Training shall be defined as one or more discussions about one function within the Software, where the total discussion time exceeds one (1) hour.
ii. End User support, or support to any person other than the five named administrators.
iii. Troubleshooting or resolution of hardware, software, security, or network-related issues on CLIENT servers or workstations.
iv. Project management support, including administration of CLIENT funding and project reports to CLIENT.
v. Courseware support, including loading of content into the site, troubleshooting issues with third party or client developed courseware, or troubleshooting user or browser configuration or related issues with viewing courseware.
vi. Integration with CLIENT applications (such as Active Directory, HRIS, or others).
vii. Database (or Environment) refreshes from CLIENT Meridian hosted Production environment(s) back to CLIENT Meridian hosted pre-production environments.

g. Credit Request and Payment Procedures.

In order to receive a credit for system availability as defined in Section 28b herein, CLIENT must make a request therefore by sending an email message to creditrequest@meridianks.com. Each request in connection with this Schedule must include CLIENT 's account number (per MERIDIAN 's invoice) and the dates and times of the unavailability of CLIENT's Web site and must be received by MERIDIAN within ten (10) business days after CLIENT's Web Site was not available. If the unavailability is confirmed by MERIDIAN, credits will be applied within one week after MERIDIAN's receipt of CLIENT's credit request.

Notwithstanding anything to the contrary herein, the total amount credited to CLIENT in a particular month under this Service Level Agreement shall not exceed the total Subscription fee paid by CLIENT for such month for the affected Services. Credits are exclusive of any applicable taxes charged to CLIENT or collected by MERIDIAN and are CLIENT 's sole and exclusive remedy with respect to any failure or deficiency in the Availability of Service.

29. Survival

In the event of any termination of the Agreement, Sections 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, and 29 shall survive and continue in effect.

SIGNATURE PAGE FOLLOWS

MERIDIAN:	CLIENT:
MERIDIAN KNOWLEDGE SOLUTIONS, LLC,	<CLIENT_LEGAL_NAME>
a Virginia, limited liability company	a <CLIENT_STATE_FULL>, <CLIENT_TYPE_OF_COMPANY>
By:	By:
Printed Name:	Printed Name:
Title:	Title:
Date:_____	Date: _____

SCHEDULE 1
IMPLEMENTATION SERVICES SET UP AND OPTIONAL SERVICES
STATEMENT OF WORK # SOW-001

This Schedule One (1) Statement of Work ("SOW") defines the implementation Services being provided by MERIDIAN to CLIENT under the terms and conditions of the Software as a Service and Subscription Agreement; in order to enable MERIDIAN to deliver and CLIENT to receive those Software Services; and is executed by and between MERIDIAN and CLIENT.

A. Summary of Scope Implementation Professional Services

1. Standard Deliverable Summary

Meridian LMS software will be delivered to CLIENT preconfigured with standard settings derived from best practices. CLIENT will be provided a limited set of software configurable options that can be personalized to enable the software to meet their business needs (i.e. SCORM settings, Virtual meeting setup, domain configurations). MERIDIAN will (1) work with CLIENT to determine how these options should be configured and (2) implement each option based on the set of configurable parameters inherent to the software. Configuration will be limited to the product capabilities outlined in the current version of the MERIDIAN manuals and documentation as well as the scope defined herein.

The following table summarizes the software setup tasks that MERIDIAN will provide on a <SOW_FFP_OR_T&M> basis. Details and scope of these services are further defined in Section B herein.

Standard Software Setup Tasks	
Installation of Meridian LMS Environments	Discovery Session/Joint Requirements Development (JRD)
Configuration & Branding Application	Functional/Technical Consulting
System Integration	Production Installation
Training	Go Live Support
Optional Software Setup Tasks	
Historical Data Migration	. Single Sign-On
. E-Commerce Integration	. Meridian Social
. Meridian Mobile	. AdHoc
. Additional Training	

2. Change Control

CLIENT acknowledges and agrees that a fundamental guiding principle for planning and executing this process, including the establishment of the User requirements, will be the utilization of existing functionality of the Meridian LMS application on an out of the box basis. This functionality will be used to implement and deploy the requirements as defined herein and further by the Requirements documentation to be mutually developed and approved with the CLIENT. The estimated consulting fees and the planned schedule are based on this principle. The purpose of the Change Management process is to ensure that requests for Project changes (to requirements or software configuration) are properly recorded, evaluated/assessed, properly dispositioned, and incorporated into the software implementation scope as required, and schedules with the proper priority and deliverable due dates.

B. Scope Details

MERIDIAN will setup CLIENT's solution according to the following in-scope details. Each task is documented below, along with the MERIDIAN and CLIENT deliverables associated with each task, assumptions, and the acceptance criteria.

Any additional configurations, or e-learning consulting by MERIDIAN, outside the scope defined herein, can be performed by:

a. MERIDIAN Professional Services on a fixed fee or time and materials basis under a separate change request, or
b. CLIENT upon the completion of MERIDIAN Administration training.

MERIDIAN offers its Direct Labor Rates as depicted herein. Cost estimates for any additional services will be provided to CLIENT upon CLIENT'S request. Upon execution of the Schedule 2 Change Order, defining the additional work to be performed, associated cost and any other relevant information, MERIDIAN will commence work.

1. Standard Setup Tasks: Installation of Meridian LMS Environments

The purpose of this task is to establish the Meridian LMS pre-production environments that support the software implementation lifecycle as outlined further in this SOW and ensure configuration management between software environments.

The following software environments will be installed with out of the box settings as part of this task.

Meridian LMS Environments	
Development **(Internal – MERIDIAN access only)**	MERIDIAN'S Development Environment is an environment that is utilized for testing all product extensions efforts, specifically the initial integration of

	subcomponents and object classes after development by the MERIDIAN developers on a local machine.
Quality Control **(Internal – MERIDIAN access only)**	MERIDIAN's Quality Control Environment is utilized for functional and technical testing to ensure quality of the development and configuration settings as aligned to CLIENT approved requirements, prior to release to CLIENT for testing activities.
Stage **(External)**	MERIDIAN'S Staging Environment is an environment that is utilized to setup the CLIENT software based upon scope defined herein. The Stage environment is available for CLIENT Acceptance Testing, allowing project participants and stakeholders to log in and review overall functionality, implementation configurations, product extensions, and integrations that are applicable.

MERIDIAN Deliverables	CLIENT Deliverables
Establish Development, Quality Control, and Stage environment described as aforementioned under section 1. Provide Client project manager URL, login, and password to stage environment. Provide system baseline documentation.	Confirmation of receipt of URL and access to the stage environment.
Assumptions	**Acceptance Criteria**
Additional pre-production environments are not included in this effort. CLIENT will report access to the Stage environment within three (3) days of receiving the access information.	Client receipt of stage environment credentials and confirmed access. Receipt of baseline documentation.

2. **Standard Setup Tasks: Discovery Session/Joint Requirements Development (JRD)**
   The purpose of this task is for the facilitation of the Discovery/Joint Requirements Development Session to establish Meridian LMS application branding, system configurations, and integrations. Furthermore, this session provides high level business process mapping to the Meridian LMS application.

MERIDIAN Deliverables	CLIENT Deliverables
Deliver one (1) day virtual session Provide software application branding checklist. Document configuration requirements in the Meridian standard Requirements Document. Rough Order of Magnitudes (ROMs) related to any scope changes or new tasks identified.	Provide proper resources as depicted herein. List of attendees, coordinate date/times, location(s), and meeting equipment needs. Participate in follow up conference calls to complete the Requirements Documentation.
Assumptions	**Acceptance Criteria**
One (1) day virtual. Use Case and Functional Requirements associated to specific integrations are not in scope.	System configuration requirements are complete and documented. Delivery of session.

3. **Standard Setup Tasks: Configuration and Branding Application**
   The purpose of this task is to configure and test the Meridian LMS software application based upon the completed and approved Requirements Document as defined in task B.2 above.

MERIDIAN Deliverables	CLIENT Deliverables
Complete the setup of all agreed upon software application configurations. Setup One (1) branded Meridian LMS CLIENT specific skin.	Graphics per branding checklist specifications.
Assumptions	**Acceptance Criteria**
Application Branding – MERIDIAN will deliver one (1) round of final pre-production skin mock up to the CLIENT for review and approval prior to setup in the Meridian LMS CLIENT Stage environment. Application Branding – MERIDIAN will deliver one (1) round of final pre-production skin review and changes upon applying to the Meridian LMS CLIENT Stage environment. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	Configurations completed and tested per the Requirements specified in task B.2 above. Meridian LMS application CLIENT Branded skin configured and tested, per the Requirements specified in task B.2 above.

4. Standard Setup Tasks: Functional/Technical Consulting

The purpose of this task is for MERIDIAN to provide sixteen (16) hours of functional consulting, and eight (8) hours of technical consulting, beyond the Workbook/Joint Requirement Session. The consulting as defined herein is limited to additional support on the base product in order to solve CLIENT specific business needs as it relates to business process mapping to the system. Functional and Technical consulting requires a MERIDIAN SME to learn the CLIENT specific business processes in order to provide recommendations on how to use the system in order to interface into existing processes, design of new processes, or leveraging system functionality in order to achieve specific goals.

MERIDIAN Deliverables	CLIENT Deliverables
Consulting hours as defined herein.	Business requirements & use cases to provide the required detail of understanding.
Assumptions	**Acceptance Criteria**
Additional hours can be added per the defined labor rate schedule. No formal document output such as workflows, requirements, or process interfaces unless accomplished within scope of hours. Hours are Firm Fixed Price and must be utilized, if required, within the duration of the project.	Exhaustion of the defined number of hours.

5. Standard Setup Tasks: System Integration

The purpose of the following task is to setup the inbound to Meridian LMS HRIS Integration. The HRIS inbound feed transmits employee detail from CLIENT's HR system to MERIDIAN (e.g. Employee Name, Organization, Job Title, etc.).

CLIENT will provide three (3) flat files to MERIDIAN, in MERIDIAN's format, for the inbound processing and loading of HRIS data (Organizations, Job Titles, User data). The HRIS/DAILY FEED data (flat files) must follow the specifications designated in MERIDIAN's HRIS templates. Any extension of the file schema's and/or processing/validation requirements may result in an expansion of scope for this task and may require additional funding. Meridian's tool to process the aforementioned flat files performs the appropriate inserts and updates of Organization Data, Job Titles, then Users, processing all data through the native API's of Meridian LMS.

MERIDIAN Deliverables	CLIENT Deliverables
MERIDIAN Base HRIS template Configuration of the Meridian LMS HRIS Tool based upon the completed Requirements Document specified in task B.2 above. One pre-production load of a subset of CLIENT production ready data for CAT purposes. One production load of full user data into the CLIENT production environment.	Backfill and delivery of the three (3) flat files to Meridian for processing: User Data, Organizations, Job Titles.
Assumptions	**Acceptance Criteria**
One way HRIS integration inbound to the Meridian LMS application only. Meridian configure the HRIS and load a subset of CLIENT production ready user data in the Meridian LMS CLIENT Stage environment for testing purposes. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein. Upon completion of CAT, MERIDIAN will load a full set of CLIENT production data in the Meridian LMS CLIENT production environment.	HRIS Tool configured and tested per the Requirements specified in task B.2 above, in the Meridian LMS CLIENT Stage environment. One (1) final data load in Meridian LMS CLIENT Production environment.

6. Standard Setup Tasks: Production Installation

The purpose of this task is to complete the installation of the Meridian LMS base application, database, configurations, branding and integrations into the Meridian LMS CLIENT production environment.

MERIDIAN Deliverables	CLIENT Deliverables
Meridian LMS CLIENT production base code and database installation MERDIAN will apply applicable configurations, branding, and integrations.	Validation Meridian LMS CLIENT Production install is completed per the Requirements specified in task B.2 above.
Assumptions	**Acceptance Criteria**

Limited to the installation of the application and database of one instance of the Meridian LMS CLIENT production environment. Technical support does not extend to other software or hardware support, data integration/migration or the resolution of base product issues. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	Meridian LMS CLIENT Production application has been installed and is accessible per the Requirements specified in task B.2 above.

7. Standard Setup Tasks: Training

The purpose of this task is to provide Implementation Readiness and Administrative training during the project implementation. The description of these trainings and the number of respective days is provided below.

Training Types Definitions

- Implementation Readiness Training (IRT) – two (2) days – The purpose of IRT is to level set terminology and provide core system concepts and features as it relates to key decisions that will be required during the Discovery/Joint Requirements Development Session.
- Administrative – three (3) days – The purpose of Administrative training is to provide the in-depth knowledge necessary to support administration system features and functions for the set up and management of the Meridian LMS.

MERIDIAN Deliverables	**CLIENT Deliverables**
Conduct required training sessions as depicted herein. Printed Student Guides for up to twelve (12) people.	Provide list of trainees, location(s), and training equipment in order to facilitate a hands-on training and demonstration of product features and functionality. Pre-approval of travel reimbursement, if onsite instructor led training is required.
Assumptions	**Acceptance Criteria**
No more than twelve (12) people. Travel costs are not included in the cost.	Delivery of the scoped number of days of training by type.

Implementation Readiness Training is provided prior to the Discovery/Joint Requirements Session. Administrative Training is typically provided towards the end of the implementation schedule, prior to the Customer Acceptance Testing initiation; but can be mutually agreed upon. A minimum of two (2) weeks' notice is required prior to the scheduling of training in order to appropriately manage resource schedules and minimize travel costs/impacts. End User Training is not provided within the current scope of services. Train-the-Trainer Training is not provided within the current scope of services. Technical Training is not provided within the current scope of services.	

Training Cancellation Policies.

Rescheduling or cancellations may result in a cancellation fee per the following schedule, plus any reasonable and necessary expenses incurred as a result of preparing to deliver the training described herein. Notification of a cancellation or reschedule must be made to MERIDIAN in writing.

- More than 20 business days prior to training – 0% of standard Training fee
- 11-20 business days prior to training start – 25% of standard Training fee
- 6-10 business days prior to training start – 50% of standard Training fee
- 0-5 business days prior to training start – 100% of standard Training fee

8. Standard Setup Tasks: Go-live Support

The purpose of this task is to provide CLIENT support from the initial deployment of configurations, branding, and integrations into the Meridian LMS CLIENT Production environment. This period allows the CLIENT to validate that Meridian LMS application containing all configuration, and integrations into the Production environment. Furthermore, it is the period in which the CLIENT is to finalize administrative configuration settings, new course and content readiness.

MERIDIAN Deliverables	CLIENT Deliverables
Delivery of final branding, configurations, and integrations into the Meridian LMS CLIENT Production environment.	Final sign-off on the delivery of the respective deliverables as stated in task B herein, by MERIDIAN.
Assumptions	**Acceptance Criteria**
Go live support consist of ten (10) business days' worth of implementation resource support post completion of the initial deployment into the Meridian LMS CLIENT Production environment. Extension of the Go Live task as defined herein will require additional funding.	Completion of ten (10) business day's duration beyond the completion of the initial deployment into the Meridian LMS CLIENT Production environment.

9. Optional Setup Tasks: Historical Data Migration

The purpose of this task is to provide a Data Migration with the standard Meridian LMS implementation services as depicted herein. The Legacy Data Migration (migration of user historical transcript data to Meridian LMS), Meridian will support a one-way, inbound, one-time Production data migration to import historical data based on the maximum record set of up to 100,000 records.

MERIDIAN Deliverables	CLIENT Deliverables
MERIDIAN Base Data Migration template. Configuration of the Meridian LMS HRIS Tool based upon the completed Requirements Document specified in task B.2 above. One pre-production load of a subset of CLIENT production ready data for CAT purposes. One production load of full user data into the CLIENT production environment.	Backfill and delivery of the one (1) flat file to Meridian for processing: User Data, Transcripts.
Assumptions	**Acceptance Criteria**

One way inbound Data Migration into the Meridian LMS application only. CLIENT cannot change the format of the Data Migration XLS file template. Meridian will load a subset of CLIENT production ready historical data in the Meridian LMS CLIENT Stage environment for testing purposes. Content is not included in-scope. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein. Upon completion of CAT, MERIDIAN will perform a one-time full data load of CLIENT production data in the Meridian LMS CLIENT production environment.	Data Migration completed and tested per the Requirements specified in task B.2 above, in the Meridian LMS CLIENT Stage environment. One (1) final data load in Meridian LMS CLIENT Production environment.

10. Optional Setup Tasks: Single Sign-On

The purpose of this task is to provide an Active Directory or SAML integration with the Meridian LMS implementation. Setup is limited to the Meridian LMS application out-of-the-box solution for the integration of Microsoft Active Directory services/LDAP/SAML 2.0.

MERIDIAN Deliverables	CLIENT Deliverables
If Active Directory or LDAP: Map Active Directory (AD) accounts to Meridian LMS using “sAMAccountName” or other unique identifier. Establish service to query AD. Configure IPsec tunnel. If SAML 2.0: Configure SAML Assertion Authentication Configure digital certificate for SAML signature validation. Configure SSL certificate for Meridian LMS site.	If Active Directory or LDAP: Provide remote access and credentials to access AD/LDAP for application Business Logic to query for authentication. Validate AD access in Meridian LMS CLIENT Stage and Production environment SAML 2.0: Provide SAML Authentication environment Provide digital certificate to enable SAML digital signature on Meridian LMS hosting server. Provide SSL certificate to enable secured communication between Meridian LMS and Authentication provider. Validate SAML access in Meridian LMS CLIENT Stage and Production environment.
Assumptions	**Acceptance Criteria**

Alternate or multiple Directory Services are out of scope. Single Sign-On mechanism must be utilized/enforced across all domains. SAML 2.0 Assertion integration assumes user accounts already exist in Meridian LMS and UID attributes of SAML assertion properly maps to the Meridian LMS Login ID. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	AD/LDAP/SAML integration/access validated in Meridian LMS CLIENT Stage and Production environments; and per the Requirements specified in task B.2 herein.

11. Optional Setup Tasks: eCommerce Integration

The purpose of this task is to provide E-Commerce integration with the Meridian LMS implementation. The Meridian LMS application has native and standard integration capabilities with CyberSource's e-commerce engine. Meridian will support the configuration and setup of this integration (CyberSource solution) to work with Client's respective merchant account.

MERIDIAN Deliverables	CLIENT Deliverables
Configuration of the Meridian LMS application e-Commerce functionality with Client's CyberSource account (one (1) Payment Gateway only).	Provide MERIDIAN with the applicable Merchant Account credentials. (CyberSource).
Assumptions	**Acceptance Criteria**
CLIENT will provide MERIDIAN with the Merchant Account credentials to support the required configurations of the Merchant Account to be used/integrated with the Meridian LMS application's e-commerce functionality. Limited to one (1) payment Gateway only: Cybersource. Any other Payment vendors requiring integration are not covered under this scope of work.	CLIENT validation of a successful transaction of purchase through e-commerce functionality into the live Merchant account. Confirmation that the e-commerce. functionality has been correctly configured and is functioning with Customer's account information, and in the Requirements specified in task B.2 herein.

MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	

12. Optional Setup Tasks: Meridian Social

The purpose of this task is to install and setup the standard Meridian Social module for the CLIENT. Setup is limited to the Meridian LMS out-of the-box solution for the Meridian Social module that includes supported features of the 3rd party integration.

MERIDIAN Deliverables	CLIENT Deliverables
Configuration of the Meridian LMS application.	Provide MERIDIAN confirmation of functionality is configured within Stage/Production environments.
Assumptions	**Acceptance Criteria**
Functionality setup is limited to the base solution. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	CLIENT validation of the access of the Social functionality via Meridian LMS user interface. Confirmation that the Meridian Social functionality has been correctly configured and is functioning per the Requirements specified in task B.2 herein.

13. Optional Setup Tasks: Meridian Mobile

The purpose of this task is to install and setup the standard Meridian Mobile module for the CLIENT. Setup is limited to the Meridian LMS out of the box solution for the Mobile module that includes one branded application.

MERIDIAN Deliverables	CLIENT Deliverables
Configuration of the Meridian LMS application. One Branded Application.	Provide MERIDIAN with the applicable iTunes and Google accounts for the application to be published. Provide MERIDIAN confirmation of functionality is configured within Stage/Production environments.
Assumptions	**Acceptance Criteria**
CLIENT to provide credentials for iTunes and Google to upload the application. If client desires to publish the application, this is recommended. Functionality setup is limited to the base solution.	Confirmation that the Meridian Mobile functionality has been correctly configured and is functioning per the Requirements specified in task B.2 herein.

MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	

14. Optional Setup Tasks: AdHoc

The purpose of this task is to install and setup the standard AdHoc reporting module for the CLIENT. Setup is limited to the Meridian LMS out of the box solution for AdHoc module that includes identified base product views and data object relationships.

MERIDIAN Deliverables	CLIENT Deliverables
Configuration of the Meridian LMS application.	Provide MERIDIAN confirmation of functionality is configured within Stage/Production environments.
Assumptions	**Acceptance Criteria**
CLIENT to configure desired base/custom views and database object relationships through configuration console that are not currently exposed via the identified base product views. MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	Confirmation that the Meridian AdHoc functionality has been correctly configured and is functioning per the Requirements specified in task B.2 herein.

15. Optional Setup Tasks: Training

The purpose of this task is to provide additional training during the project implementation, based upon additional standard modules, or features implemented, per the scope defined herein. The description of these trainings and the number of respective days is provided below. Training can be purchased at a fixed fee of $ per day.

Training Types Definitions

- Ad Hoc Report: (not in scope) - The purpose of this Ad Hoc Report training is to provide guidance on how to configure the Ad Hoc Report Builder and create custom reports.
- Train-the-Trainer: (not in scope) - Training to train Client Trainers on the effective ways to train the system to End Users and various audiences.
- Technical: (not in scope) - Training on how to manage integration with the Meridian system.
- End User: (not in scope) - Training for end users on how to access the system, general navigation, and feature set review.

- Additional Administrative: (not in scope) – The purpose of Administrative training is to provide the in-depth knowledge necessary to support administration system features and functions for the set up and management of the Meridian LMS.

MERIDIAN Deliverables	CLIENT Deliverables
Conduct required training sessions as depicted herein. Printed Student Guides for up to twelve (12) people.	Provide list of trainees, location(s), and training equipment in order to facilitate a hands-on training and demonstration of product features and functionality. Pre-approval of travel reimbursement, if onsite instructor led training is required.
Assumptions	**Acceptance Criteria**
No more than twelve (12) people. Travel costs are not included in the cost. A minimum of two (2) weeks' notice is required prior to the scheduling of training in order to appropriately manage resource. schedules and minimize travel costs/impacts. End User Training is not provided within the current scope of services. Train-the-Trainer Training is not provided within the current scope of services. Technical Training is not provided within the current scope of services.	Delivery of the scoped number of days of training by type.

Training Cancellation Policies.
Rescheduling or cancellations may result in a cancellation fee per the following schedule, plus any reasonable and necessary expenses incurred as a result of preparing to deliver the training described herein. Notification of a cancellation or reschedule must be made to MERIDIAN in writing.

- More than 20 business days prior to training – 0% of standard Training fee.
- 11-20 business days prior to training start – 25% of standard Training fee.
- 6-10 business days prior to training start – 50% of standard Training fee.
- 0-5 business days prior to training start – 100% of standard Training fee.

C. Project Schedule

The scope of the implementation services as depicted herein is limited to a one (1) phase software deployment, estimated to take sixteen (16) weeks.
Schedule is dependent on CLIENT's ability to:

1. Complete all Discovery and Planning activities per the mutually agreed upon baselined Project Plan, including but not limited to:
   a. Data Template Completion
2. Provide Configuration and Integration Requirements in a timely manner.
3. Provide feedback on all loaded data in a timely manner
4. Execute Customer Acceptance Testing activities per the agreed upon Project Plan

A draft Project Plan will be provided within one (1) week after the Project Kick-Off date. The detailed Project Plan is subject to modification during the software implementation lifecycle with the mutual agreement of both the CLIENT and MERIDIAN.

D. Roles and Responsibilities

MERIDIAN and CLIENT agree to staff the Project at levels and conditions as set forth in the mutually agreed upon Project Plan. At a minimum, across all tasks as defined in section B.2 above, the Project will be staffed as follows:

MERIDIAN Resources

Role	Responsibilities	Participation	Skill Set
Project Manager	Acts as Meridian's single point of contact throughout the project. Develops and manages project plan. Manages project issues and mitigates risk on behalf of Meridian. Prepares for and conducts status meetings Provides status reports and financial tracking. Conducts Requirement Confirmation Workshops.	Deployment Stages. Discovery. Execute. Deploy. Warranty. Workstreams Project Management. Software Setup.	Project Management experience managing teams, issues, project schedules and financials. Meridian LMS configuration skills. Process definition skills.

	Participates in and coordinates design, configuration, development, testing and deployment activities. Note: In most cases, the Meridian Project Manager is not fully dedicated to one specific customer deployment since the responsibility does not require a full-time resource.	Meridian University.	
Technical Solutions Architect	Conduct Requirement Confirmation workshops to gather in-scope product extension requirements for complex projects only. Drives the joint project team to a solution to meet all requirements in the most efficient and constructive manner. Participates in execution of software development and testing activities.	Deployment Stages. Discovery. Execute. Warranty. Workstreams. Software Setup.	Meridian LMS product features & functionality expert. Industry Business Process expert. SQL database skills. SQL query skills. Process definition skills. Data analysis skills. Data conversion skills.
Implementation Consultant	Facilitates end-user and system admin Requirements Gathering Sessions. Confirms configuration requirements.	Deployment Stages. Discovery. Execute. Deploy. Warranty.	Meridian LMS product configuration skills. In-depth Industry and process knowledge. SQL query skills. Process definition skills.

	Identifies gaps and works with integrated team to develop resolutions. Performs data conversion and migration activities. Configures and tests software per defined requirements.	Workstreams. Software Setup.	Data analysis skills.
Application Developer	Establishes technical environments. Extends software for requirements not supported by out-of-the-box features & configurations. Configures/Develops integrations with the product per defined requirements.	Deployment Stages. Discovery. Execute. Deploy. Warranty. Workstreams. Software Setup.	Meridian LMS development expert. SQL database skills. SQL query skills. .NET development skills. Meridian LMS technical infrastructure skills.
Account Manager	Analyzes and assesses client's maturity level and skill sets. Assesses client's business processes and goals. Creates recommendations to drive the maturity and the business forward. Establishes and tracks strategic initiatives.	Workstreams. Post Deployment.	In-depth Industry knowledge. In-depth knowledge of industry best practices. Strategic planning. Project/Account Management. Process definition and development skills. Enablement and communications expert.

Meridian Trainer	Delivers Implementation Readiness and LMS Administrator training. Tailors training delivery to meet customer's business requirements and/or configuration decisions. Finalizes training logistics.	Deployment Stages. Discovery. Execute. Workstreams. Meridian University.	Meridian LMS product features and functionality expert. In-depth knowledge of industry best practices.

E. Cost Estimate

Item Description	Cost
Standard Software Setup	$
Installation of Meridian LMS Environments	Included
Discovery Session/Joint Requirements Development (JRD)	Included
Configuration & Branding Application	Included
Functional/Technical Consulting	Included
System Integration	Included
Production Installation	Included
Training	Included
Go Live Support	Included
Optional Software Setup Tasks	$XXXXXXXXX
Historical Data Migration	$
Single Sign-On	$
eCommerce Integration	$
Meridian Social Setup	$
Meridian Mobile	$
AdHoc Setup	$
Additional Training	$/Day

COST ASSUMPTIONS:

1. All Services are an estimate based on the understanding of the scope of work. Implementation Services may vary based on increased domains, user audience, and scope, or time changes. Any additional Services that are identified through the workbook process (additional modifications, integrations, professional services support or consulting) can be added to this Agreement as needed or in a later CO SOW.
2. All pricing for additional scopes of work is valid for ninety (90) calendar days from the date of submission to the CLIENT.
3. Travel costs are not included in the Cost Estimate and will be invoiced per MERIDIAN'S current travel guidelines.

F. Out of Scope

The following is currently deemed outside of the scope for this implementation:
Migrations, integrations, modifications to the system that are not explicitly included in the scope of this SOW.

i. Custom reports, localization, documentation, or online help.
ii. Content cleansing, migration, or uploading unless specifically identified.
iii. Consulting or professional services not specified in the implementation tasks (i.e. courseware development, courseware troubleshooting, SCORM, HW/SW configurations or internal network setup or maintenance.)
iv. Advanced Graphical design or other advanced (e.g. flash) GUI support.
v. Editable training materials such as instructor and student guides.

G. Change Management

MERIDIAN recognizes that changes are a normal part of the project life cycle. Changes to the scope or timeline of the Services contemplated by this Agreement will require a formal Change Order Statement of Work ("Schedule 2") to be submitted by the MERIDIAN Project Manager to the CLIENT. Changes in scope may include an increase in cost and/or timeline and will be specified in each change request. Prior to beginning the change request, CLIENT must execute the Schedule 2 Change Order. MERIDIAN requires formal change acceptance before beginning work on any changes. Changes within the defined scope of the contract need approval by the CLIENT Project Manager and the MERIDIAN Project Manager. Acceptance for scope changes, are given when both the CLIENT Project Manager and the MERIDIAN Project Manager formally approve the change by signing off on Schedule 2 so that miscommunications are avoided. Project change procedure is as follows:

i. Identify change (can originate from the CLIENT Project Manager or the MERIDIAN Project Manager);
ii. MERIDIAN completes Change Request Form;
iii. MERIDIAN Project Manager determines the impact of the proposed change (schedule, resources, time, and/or cost);

iv. MERIDIAN Project Manager submits Schedule 2 to the CLIENT Project Manager for review/approval.
v. MERIDIAN Project Manager receives approval from the CLIENT Project Manager within three (3) business days; and
vi. MERIDIAN Project Manager modifies or, if necessary, re-baselines the Project Schedule and Plan to include the approved change.
vii. Work begins as agreed upon to incorporate change; or,
viii. MERIDIAN Project Manager works with the CLIENT Project Manager to either adjust the requirements or revise the workload distribution, documenting all changes on a revised Change Request Form.

Change Management Criteria are as follows:

iv. Any change that is outside the scope of effort defined in Schedule 1;
v. Any additional deliverable or service not defined in Schedule 1, or changes to an accepted deliverable;
vi. Any subsequent modifications to an approved Change Request;
vii. Modifications to the technical or management approach defined in Schedule 1;
viii. Any change in workload or environment or application inventory;
ix. Any additional activity or task not defined in Schedule 1 for a planned deliverable;
x. A contradiction to items, assumptions or responsibilities stated in Schedule 1;
xi. A delay in turnaround of approvals, information, answers to questions; and
xii. Time lost due to reasons such as unavailability of equipment, software, or access to environment/infrastructure needed by the project team.

H. Acceptance Management

In an effort to avoid schedule delays stemming from delayed approvals of dependent tasks, MERIDIAN and CLIENT will mutually define a reasonable acceptance review period that does not jeopardize the project duration as outlined within the project management support period. Delays in accepting project deliverables could result in a schedule slippage equaling as much as one day for every day acceptance review is delayed. Below are the methods used to verify and validate each of the defined deliverable(s).

i. **Deliverable Review and Approval.** MERIDIAN will provide deliverables to the CLIENT. Documentation deliverables will be provided to CLIENT in electronic form. A Deliverable Acceptance Form will be submitted to the CLIENT Project Manager for each deliverable. CLIENT will provide MERIDIAN with one set of consolidated comments. MERIDIAN will provide a CLIENT Quality Control (QC) sheet that may help the CLIENT collate all comments prior to delivering to MERIDIAN. The deliverable will be deemed acceptable when it satisfies the acceptance criteria specified for each deliverable or service or within ten (10) calendar days if no response is received. The Deliverable Acceptance will be signed and returned to MERIDIAN upon review of the deliverable within the mutually defined period as stated upon under acceptance

management. In the event that the CLIENT rejects a deliverable, MERIDIAN will resubmit the deliverable to the CLIENT with the required changes within a mutually agreed upon timeline.

ii. **Acceptance Authority.** CLIENT will specify a single point of contact with deliverable acceptance/sign off authority. Sign off acceptance is required for deliverable by the approving authority, prior to moving any customizations to the production site.

iii. **Withholding Acceptance.** CLIENT shall not unreasonably withhold acceptance. If Acceptance is not granted or rejected within the mutually agreed upon timeframe, automatic Acceptance will be granted. In the event that failure to provide Acceptance extends the timeframe of the implementation activities within the respective Schedule 1, CLIENT may be liable for additional Project Management time in order to extend the schedule.

iv. **30 Day Post-Delivery Warranty.** After sign-off approval has been received, and MERIDIAN has delivered the files, CLIENT will have thirty (30) calendar days in which to report any production errors to the Project Manager. MERIDIAN will assess the error and correct as long as the error is within the scope of the original task completed. After thirty (30) calendar days from the date the files were delivered to the CLIENT, MERIDIAN will provide a cost estimate for any errors/revisions requested unless those costs are covered under separate sections of this Agreement. This warranty is only in terms of the work performed under the Exhibit A.

I. Invoicing Schedule

MERIDIAN will invoice Services based on the following deliverable milestones within the implementation timeline.

i. **Contract Execution [20%]** – Upon Contract Execution, twenty percent (20%) of the SOW fee will be invoiced.

ii. **Delivery to CLIENT Stage Environment [35%]** – At the point of all programmatic deliverables being released to the CLIENT Stage Environment for CLIENT review, the second thirty-five percent (35%) of the SOW fee will be invoiced.

iii. **Delivery to Production [35%]** – At the point of all programmatic deliverables being delivered for application to the Production Environment, thirty-five percent (35%) of the SOW fee will be invoiced.

iv. **Warranty Period Complete [10%]** – At the completion of the thirty (30) calendar day warranty period, the remaining ten percent (10%) of the SOW fee will be invoiced.

J. Additional Services – Labor Rates - RESERVED

K. Authorization

By signing below, CLIENT is authorizing MERIDIAN to move forward with the development and testing of the requested functionality, as detailed within this document. CLIENT agrees that the

requirements, as documented herein, meet or exceed the expectation of the requested functionality.

Once signed, this page should be faxed or emailed to Meridian Knowledge Solutions, LLC:

To the attention of:	Contracts
Fax #:	703.322.9568
Email	contracts@meridianks.com

MERIDIAN: MERIDIAN KNOWLEDGE SOLUTIONS, LLC, a Virginia, limited liability company	CLIENT: <CLIENT_LEGAL_NAME> a <CLIENT_STATE_FULL>, <CLIENT_TYPE_OF_COMPANY>
By: Printed Name: Title: Date: _____	By: Printed Name: Title: Date: _____

SCHEDULE 2
SOFTWARE AS A SERVICE AND SUBSCRIPTION AGREEMENT

CHANGE ORDER TO SCHEDULE 1 - STATEMENT OF WORK #CO-001 (TEMPLATE)
IMPLEMENTATION OF THE MERIDIAN LMS
FOR <CLIENT_LEGAL_NAME>

This Schedule 2 is a Change Order to Schedule 1 – Statement of Work # SOW-001, dated <SOW_EFFECTIVE_DATE_MM/DD/YYYY>, and defines changes to the work to be provided under the terms and conditions of the Contract Agreement signed between MERIDIAN and CLIENT.

L. Effective Date of this Schedule 2

This Change Order is effective upon its execution by MERIDIAN and CLIENT. The estimated Change Order commencement date is <CHANGE_ORDER_EFFECTIVE_DATE_MM/DD/YYYY>.

M. Summary of Changes to the Scope of Implementation Professional Services

CLIENT has requested the following changes to the LMS implementation in support of **<add detail as needed>**.

A. Authorization

By signing below, CLIENT is authorizing MERIDIAN to move forward with the development and testing of the requested functionality, as detailed within this document. CLIENT agrees that the requirements, as documented herein, meet or exceed the expectation of the requested functionality.

Once signed, this page should be faxed or emailed to Meridian Knowledge Solutions, LLC:

To the attention of:	Contracts
Fax #:	703-322-9568
Email	contracts@meridianks.com

SIGNATURE PAGE FOLLOWS

MERIDIAN: MERIDIAN KNOWLEDGE SOLUTIONS, LLC, a Virginia, limited liability company	CLIENT: <CLIENT_LEGAL_NAME> a <CLIENT_STATE_FULL>, <CLIENT_TYPE_OF_COMPANY>
By: Printed Name: Title: Date: _____	By: Printed Name: Title: Date: _____

General Terms and Conditions

This Software as a Service Subscription Agreement (this "Agreement") is made and entered into as of the effective date set forth below (the "Effective Date") between:

Effective Date of this Agreement: <EFFECTIVE_DATE_MM/DD/YYYY>

MERIDIAN:	**CLIENT:**
MERIDIAN KNOWLEDGE SOLUTIONS, LLC, a Virginia, limited liability company	**<CLIENT_LEGAL_NAME> a <CLIENT_STATE_FULL>, <CLIENT_TYPE_OF_COMPANY>**

THESE TERMS AND CONDITIONS CONSTITUTE THE ENTIRE LEGAL AGREEMENT BETWEEN CLIENT AND MERIDIAN KNOWLEDGE SOLUTIONS, LLC ("MERIDIAN") CONCERNING THE ACCESS TO THE PROPRIETARY MERIDIAN LMS SOFTWARE PROGRAM, ASSOCIATED DOCUMENTATION ("Software") AND THE SERVICES PERFORMED BY MERIDIAN IN SUPPORT THEREOF.

A. MERIDIAN has developed certain software programs and associated documentation which MERIDIAN makes available to its CLIENT's ("Subscribers") on a Subscription ("Subscription") basis.

B. CLIENT wishes to use MERIDIAN'S Services and Software in its business operations.

C. MERIDIAN has agreed to provide, and the CLIENT has agreed to pay for and use MERIDIAN'S Services and Software subject to the terms and conditions of this Agreement.

D. In the event there are conflicting terms among the various documents, the order of precedence is as follows: 1) This Agreement; 2) Project Documents; and 3) Exhibit(s).

1. Definitions

a. Authorized User: Employees, agents, and independent contractors of the CLIENT who are authorized to use the Software as described herein.
b. Confidential Information: Information that is proprietary or confidential of MERIDIAN as further defined throughout this Agreement.
c. CLIENT Data: Data that is input by the CLIENT or Authorized Users of the CLIENT into the Software for the purpose of utilizing the Software.

d. Documentation: Documents made available by MERIDIAN to the CLIENT from time to time which may include but is not limited to documents containing Software descriptions, user manuals and other material related to the Software.
e. Effective Date: The day this Agreement takes effect.
f. Initial Subscription Term: The initial term of this Agreement.
g. Internal Business Operations: The internal business processes of an organization. Business operations include the day-to-day activities of the business. Such operations facilitate the achievement of a business' prime function.
h. Standard Business Hours: Monday through Friday 8 am – 8 pm Eastern Standard Time (EST).
i. Services: The access to the software services (Software Services, Implementation Services, collectively, and any Support provided for such Services) provided by MERIDIAN to CLIENT under this Agreement.
j. Software: The application provided as a part of the Services Subscription.
k. Subscription Fees: The fees payable to MERIDIAN by the CLIENT for the User Subscriptions.
l. Subscription Term: The term of the Subscription.
m. Support: The general maintenance and technical support Services as set forth herein.
n. Support Policy: MERIDIAN'S policy for providing support in relation to the Services as described herein
o. Service Levels: The Service Level commitments as set forth herein.
p. User Subscription: The subscriptions purchased to grant Authorized Users access to the Services as described herein.
q. Product Extensions: Any modification to the base Meridian LMS application that is specific to the CLIENT's requirements and scope as defined in the Statement of Work and any associated Change Order. Product Extensions (also known as customizations) are prohibited in this agreement.
r. Enhancements: Any Meridian governed and deployed product change that increases or modifies the Meridian LMS functionality or feature set; and is not specific to a Client. The release and application of any product Enhancement is at the sole discretion of Meridian.
s. Software Updates: Meridian governed product updates that provide software defect resolutions for existing base Meridian LMS application features or functionality. The updates are provided in patch sets, point releases, or hot/emergency fixes (for example, Version 14.4.1 to 14.4.2). The release and application of any Software Update is at the sole discretion of Meridian.
t. Software Version Upgrades: A major, standalone version of the Meridian LMS application, and is further defined as the CLIENT moving from one major Release of the Meridian LMS application to another (for example, Version 13.0 to 14.0). Software upgrades are included in this agreement. The release and application of any Software Version Upgrade is at the sole discretion of Meridian.

2. Subscription

a. Subject to the CLIENT purchasing the User Subscription, the restrictions set forth in this Section and other terms and conditions of this Agreement, MERIDIAN hereby grants to the CLIENT, a non-exclusive, non-transferable right to permit the Authorized Users of the CLIENT to (i) use such Services; and (ii) display such Services solely for the purpose of exercising CLIENT's rights and performing CLIENT's obligations hereunder. The foregoing subscription is subject to the restrictions below and the other terms and conditions of this Agreement. Services shall be used during the Subscription Terms solely for the CLIENT's Internal Business Operations.

b. In relation to the Authorized Users, the CLIENT agrees that:
   i. the maximum number of Authorized Users that it authorizes to access and use the Services shall not exceed the number of User Subscriptions CLIENT has purchased;
   ii. CLIENT will not allow any User Subscription to be used by more than one individual Authorized User during an annual subscription term. A license can be reassigned in its entirety upon the next annual subscription term to another individual Authorized User, in which case the prior Authorized User shall be flagged inactive and no longer have any right to access or use the Services;
   iii. MERIDIAN will monitor the actual number of Authorized Users to ensure compliance with Item (2)(a)(b) above during the annual subscription term.

c. The CLIENT will not intentionally access, store, distribute or transmit any viruses, Trojans or any and all malicious code, or any material during the course of its use of the Services that as outlined below. In the event any of the identified items occur, CLIENT will remove and promptly notify MERIDIAN immediately if there is potential harm to the software.
   i. is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
   ii. facilitates illegal activity;
   iii. depicts sexually explicit images;
   iv. promotes unlawful violence;
   v. is discriminatory based on race, gender, color, religious belief, sexual orientation, disability, or any other illegal activity;
   vi. causes damage or injury to any person or property; or
   vii. infringes on third party intellectual property, copyright or trademark rights.

   MERIDIAN reserves the right, without liability to the CLIENT, to disable the CLIENT's access to any material that breaches the provisions of this clause.

d. The CLIENT shall not except to the extent expressly permitted under this Agreement:
   i. attempt to reproduce, copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute, in whole or in part, any portion of the Software and/or Documentation (as applicable) in any form or media or by any means;

ii. attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software;
iii. access all or any part of the Services and/or Documentation in order to build a product or service which competes with the Services, Software and/or the Documentation provided by this Agreement;
iv. use the Services, and/or Documentation to provide services to third parties; or
v. subject to the Assignment Section, license, sublicense, sell, rent, lease, transfer, subcontract, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services, and/or Documentation available to any third party except the Authorized Users, or
vi. attempt to obtain, or assist third parties in obtaining, access to the Services, and/or Documentation, other than as provided under this clause.

e. The CLIENT shall use all reasonable endeavors to prevent any unauthorized access to, or use of, the Services, and/or the Documentation and, in the event of any such unauthorized access or use, promptly notify MERIDIAN. The rights provided under this Section are granted to the CLIENT only, and shall not be considered granted to any subsidiary or affiliate of the CLIENT.

f. Additional User Subscriptions
i. The CLIENT may, during any Subscription Term, purchase additional User Subscriptions in excess of the number set out in Schedule 1 and MERIDIAN shall grant access to the Services to such additional Authorized Users in accordance with the provisions of this Agreement.
ii. If the CLIENT wishes to purchase additional User Subscriptions, the CLIENT shall notify MERIDIAN in writing. MERIDIAN shall evaluate such request for additional User Subscriptions and respond to the CLIENT with approval or disapproval of the request and such approval not to be unreasonably withheld.
iii. If MERIDIAN approves the CLIENT's request to purchase additional User Subscriptions, the CLIENT shall, within thirty (30) calendar days of the date of MERIDIAN'S invoice, pay MERIDIAN the relevant fees for such additional User Subscriptions as set out in Schedule 1 and, if such additional User Subscriptions are purchased by the CLIENT part way through the Initial Subscription Term or any Renewal Period (as applicable), such fees shall not be pro-rated for the remainder of the Initial Subscription Term or then current Renewal Period (as applicable).

3. Fees; Payment Terms

a. Fees. In consideration of this Agreement, CLIENT will pay the Subscription fees set forth in Section 27 (the "Subscription Fees"). In consideration of any other products provided or services performed under this Agreement, CLIENT will pay the fees and charges described in Section 27 and the applicable Schedules. On the Effective Date of this Agreement, the

Subscription Fees shall be payable with respect to the Initial Subscription Term and at least thirty (30) calendar days prior to each anniversary of the Effective Date, the Subscription Fees shall be payable with respect to the next Renewal Period. If, at any time while using the Services, the CLIENT exceeds the amount of storage space specified in Section 27, MERIDIAN shall charge the CLIENT, and the CLIENT shall pay MERIDIAN'S then current excess data storage fees. MERIDIAN'S excess data storage fees are set out in Section 27 and current as of the Effective Date. MERIDIAN shall be entitled to increase the Subscription Fees, with respect of the additional User Subscriptions purchased, and/or the excess storage fees at the start of each Renewal Period upon thirty (30) calendar days' prior notice to the CLIENT and Section 27 shall be deemed to have been amended accordingly. Fees are non-cancellable and non-refundable except as otherwise stated herein.

b. Payment. All fees and expenses will be due and payable to MERIDIAN within thirty (30) calendar days after the date of invoice. All fees and expenses will be paid to MERIDIAN in United States dollars, by wire transfer of funds to an account designated by MERIDIAN or by check sent to MERIDIAN at Attention: Accounts Receivable, Meridian Knowledge Solutions, LLC, 80 Iron Point Circle, Suite 100, Folsom, CA 95630 unless otherwise specified by MERIDIAN. All past-due payments will bear interest at the rate of one and one-half percent (1½%) per month or the maximum rate allowed by law, whichever is less. MERIDIAN shall have the right to terminate the Agreement for default/cause if the CLIENT does not pay MERIDIAN'S undisputed invoices within the terms contained herein. All outstanding invoices will be due and payable immediately upon such termination. If CLIENT does not pay MERIDIAN for any undisputed outstanding invoices, and MERIDIAN incurs any additional costs including, but not limited to court costs, attorney's fees and other damages, in the collection of said invoices, MERIDIAN shall have the right to recover the additional costs from CLIENT.

c. PCI Compliance. In the event CLIENT engages in payment card transactions as part of the services provided to MERIDIAN, CLIENT shall comply with the Payment Card Industry Data Security Standard ("CI-DSS") and any amendments or restatements of the PDI DSS during the Term of this agreement. CLIENT accepts responsibility for the security of customer credit card data in its possession, even if all or a portion of the services to MERIDIAN are subcontracted to third parties

d. Taxes. CLIENT acknowledges and agrees that it is responsible for the payment of all applicable taxes and duties, including, without limitation, sales, use, excise, value added and franchise taxes, associated with this Agreement, the products provided and the services performed under this Agreement, except for taxes based on MERIDIAN'S income.

e. The CLIENT shall on the Effective Date provide to MERIDIAN valid, up-to-date and complete approved purchase order information acceptable to MERIDIAN and any other relevant information needed by MERIDIAN to invoice CLIENT.

f. If MERIDIAN has not received payment within thirty (30) calendar days after the due date of any undisputed invoice, and without prejudice to any other rights and remedies of Meridian.

g. MERIDIAN may, without further liability to the CLIENT, disable the CLIENT's passwords, accounts and access to all or part of the Services. MERIDIAN shall be under no further obligation to provide any or all of the Services while the invoice(s) concerned remain unpaid; and MERIDIAN shall have the right to terminate the Agreement for default if the CLIENT does not pay MERIDIAN'S undisputed invoices within the terms contained herein. All outstanding invoices will be due and payable immediately upon such termination. If CLIENT does not pay MERIDIAN for any undisputed outstanding invoices, and MERIDIAN incurs any additional costs including, but not limited to court costs, attorney's fees and other damages, in the collection of said invoices, MERIDIAN shall have the right to recover the additional costs from CLIENT.

4. Proprietary Rights

a. CLIENT acknowledges and agrees that the Software is protected by U.S. and international copyright, patent, trademark, trade secret and other intellectual property rights and registrations. CLIENT acknowledges that all right, title and interest in and to the Software and all intellectual property rights thereto will be owned solely by MERIDIAN and its licensors, as applicable. CLIENT will not remove, obliterate, obscure or alter any copyright or other proprietary rights notice that appears on the Software. Except for the limited rights expressly granted to CLIENT under this Agreement, CLIENT is not granted any other rights in or to the Software. All rights in and to the Software not specifically granted herein are reserved to MERIDIAN and its licensors, as applicable.

5. Confidentiality Obligations

a. Confidential Information. "Confidential Information" means any and all information that is of a confidential, proprietary or trade secret nature that is furnished or disclosed by MERIDIAN to CLIENT under this Agreement. Without limiting the generality of the foregoing, "Confidential Information" includes the Software (including the object code and source code forms thereof), the specific business terms of this Agreement and any other information that is marked as "Confidential," "Proprietary," "Trade Secret" or in some other manner to indicate its confidential, proprietary or trade secret nature. "Confidential Information" will not include: (i) information that is or becomes publicly known through no fault of CLIENT ; (ii) information received from a third party that was disclosed without breach of any confidentiality obligation; (iii) information approved for release by written authorization of Meridian; (iv) information developed or created independently by CLIENT without reference to, or use of, MERIDIAN'S

Confidential Information; or (v) information that may be required by law, regulation or an order of any court, agency or proceeding to be disclosed, provided that CLIENT will provide MERIDIAN with written notice of any such required disclosure once CLIENT has knowledge of it and will help MERIDIAN at the expense of CLIENT to the extent reasonable to obtain an appropriate protective order.

b. Non-Disclosure. All Confidential Information will remain the property of MERIDIAN and CLIENT will not be deemed by virtue of its access to MERIDIAN'S Confidential Information to have acquired any right or interest in or to any such Confidential Information, other than as specifically set forth herein. CLIENT agrees: (i) to hold the Confidential Information in strict confidence; (ii) except as expressly authorized in this Agreement, not to disclose any Confidential Information to any third party other than employees and independent contractors of CLIENT who have a need to know the Confidential Information for the purposes of this Agreement and who are subject to a confidentiality agreement that affords at least as much protection to the Confidential Information as this Section 5; (iii) to use the Confidential Information solely and exclusively in accordance with the terms of this Agreement in order to carry out CLIENT's obligations and exercise its rights under this Agreement; and (iv) to notify MERIDIAN promptly of any unauthorized use or disclosure of the Confidential Information and to cooperate with and assist MERIDIAN in every reasonable way to stop or minimize such unauthorized use or disclosure.

c. Injunction. CLIENT agrees that if a court of competent jurisdiction determines that CLIENT has breached, or attempted or threatened to breach, its confidentiality obligations to MERIDIAN or MERIDIAN'S proprietary rights, MERIDIAN will be entitled to obtain appropriate injunctive relief and other measures restraining further attempted or threatened breaches of such obligations. Such injunctive relief or other measures will be in addition to, and not in lieu of, any other rights and remedies available to MERIDIAN.

6. CLIENT Data

a. The CLIENT shall own all rights, title and interest in and to all of the CLIENT Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the CLIENT Data.

b. MERIDIAN shall follow its commercially reasonable backup procedures for CLIENT Data and said procedure may be amended by MERIDIAN in its sole discretion from time to time based upon best practices. In the event of any loss or damage to CLIENT Data, the CLIENT's sole and exclusive remedy shall be for MERIDIAN to use reasonable commercial activities to restore the lost or damaged CLIENT Data from the latest back-up of such CLIENT Data maintained by MERIDIAN in accordance with the backup procedure described herein. MERIDIAN shall not be responsible for any loss, destruction, alteration or disclosure of

CLIENT Data caused by any third party (except those third parties subcontracted by MERIDIAN to perform services related to CLIENT Data maintenance and back-up).

c. MERIDIAN shall, in providing access to the Services, comply with its Privacy Policy relating to the privacy and security of the CLIENT Data available at http://www.meridianks.com/privacy-statement/ or such other Policy as may be given to the CLIENT from time to time, as such document may be amended from time to time by MERIDIAN in its sole discretion.

d. MERIDIAN strongly recommends that CLIENT not store or process Personally Identifiable Information (PII) or Personally Identifiable Health Information (PHI) within the Software. PII is defined as information that can be used to uniquely identify a single individual and may include an individual's name in combination with a Driver's License, Social Security Number or Credit Card Information. The definition of PII varies depending on international, federal, state and local laws and the definition contained herein shall be used for reference purposes only and shall not be construed as covering all possible definitions of PII. PHI is defined as any information that is related to an individual's health record as defined by the Health Insurance Portability and Accountability Act (HIPAA).

e. PHI/PII Processing - The parties shall comply, and warrant that they have complied, with implementing all applicable data protection and privacy laws and regulations in any relevant jurisdiction (together, the "Data Protection Laws"); and where, in connection with this Agreement, the Software is processing information related to PHI/PII on behalf of the CLIENT, MERIDIAN shall:

i. Process the PHI/PII only on the written instructions of CLIENT;
ii. Make all reasonable efforts to implement appropriate technical and organizational measures to protect those PHI/PII against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;
iii. Return or destroy all such personal data promptly upon the termination of this Agreement, or at any time during the term of this Agreement upon written instructions from CLIENT;
iv. Not disclose PHI/PII to any person except as required or permitted by this Agreement or with CLIENT's written consent;
v. Provide full cooperation and assistance to CLIENT in implementing any procedures required in order to comply with data privacy laws to which CLIENT is subject, as advised by CLIENT from time to time;
vi. Not process PHI/PII except to the extent reasonably necessary to the performance of this Agreement;

vii. Notify CLIENT immediately in the event of any breach of the security of such personal data, and cooperate with CLIENT in any post- breach investigation or remediation efforts; and

viii. Notify CLIENT promptly in the event that MERIDIAN is required by law, court order, warrant, subpoena, or other legal or judicial process to disclose any PHI/PII to any person other than CLIENT.

The CLIENT shall make all reasonable efforts to ensure that those Personal Data are accurate and up to date at all times, to the extent that it is within CLIENT's ability to do so.

The Parties hereto agree, that the above warranties relating to PHI and PII are Meridian's sole responsibilities related to the processing and control of CLIENT PHI and PII.

7. European Union Clients

In the event that CLIENT will access PII originating from a country in the European Economic Area ("EEA") or from a country outside the EEA, MERIDIAN shall, if requested by CLIENT, will comply with the applicable Privacy Law Legislation in coordination with the European Commission, relating to requirements of the European Union's Directive on Data Protection. CLIENT warrants that it has the consent of its employees, independent contractors or any other individual whose PII is being processed and/or transmitted within the Services and MERIDIAN shall have no liability should CLIENT not have received such consent. CLIENT will indemnify, defend and hold MERIDIAN harmless should any such individual or group of individuals bring any suit against MERIDIAN for violation of any applicable law.

8. Limited Warranty / Acceptance

a. MERIDIAN warrants that it will perform the Services in a manner consistent with industry standards reasonably applicable to the performance thereof. MERIDIAN does not warrant that Client's use of the Services will be uninterrupted or error free. The limited warranties set forth in this Agreement do not apply to any deviation by the Software from the specifications set forth in the applicable Schedule that is caused by, or results from, (i) improper usage of Software APIs (Application Programming Interfaces) or the introduction/import of corrupt data into the Software by anyone other than MERIDIAN; (ii) use of the Services for any purpose other than that authorized in this Agreement; (iii) use of the Services in combination with other software, data or products that are defective or incompatible with, or are not authorized by MERIDIAN for use with, the Services; (iv) any malfunction of CLIENT's software, hardware, computers or computer-related equipment; (v) CLIENT'S failure to use any Updates made available by MERIDIAN; or (vi) an event of Force Majeure (defined below).

b. MERIDIAN DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM THE SOFTWARE AND OTHER PORTIONS OF THE INTERNET. SUCH FLOW DEPENDS IN

LARGE PART ON THE PERFORMANCE OF INTERNET SERVICES PROVIDED OR CONTROLLED BY THIRD PARTIES. AT TIMES, ACTIONS OR INACTIONS OF SUCH THIRD PARTIES CAN IMPAIR OR DISRUPT CUSTOMER'S CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF). ALTHOUGH MERIDIAN WILL USE COMMERCIALLY REASONABLE EFFORTS TO TAKE ALL ACTIONS IT DEEMS APPROPRIATE TO REMEDY AND AVOID SUCH EVENTS, MERIDIAN CANNOT GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR. ACCORDINGLY, MERIDIAN DISCLAIMS ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO SUCH EVENTS.THE FOREGOING WARRANTIES ARE MADE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR COURSE OF PERFORMANCE. EXCEPT AS EXPRESSLY PROVIDED HEREIN, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH CLIENT'S ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT, THE SERVICES ARE PROVIDED "AS IS," AND MERIDIAN DISCLAIMS ANY WARRANTY AS TO THE QUALITY, OPERATION OF, ACCESS TO OR USE OF ALL OR ANY PART OF THE SOFTWARE AND ANY WARRANTY THAT (I) THE SERVICES WILL OPERATE UNINTERRUPTED OR ERROR-FREE, (II) THE RESULTS ARISING OUT OF THE USE OF THE SERVICES WILL BE ACCURATE, COMPLETE OR ERROR-FREE, OR (III) THE SERVICES WILL MEET THE NEEDS OF CLIENT OR ITS CLIENTS, AGENTS OR SUPPLIERS.

c. Acceptance of the Software will be upon the CLIENT's receipt of the URL from MERIDIAN, where CLIENT will be provided access to the Software.

9. Other CLIENT Obligations

a. The CLIENT shall provide MERIDIAN with:
   i. all necessary cooperation in relation to this Agreement;
   ii. all necessary access to such information as may be required by MERIDIAN in order to render the Services, including but not limited to CLIENT Data, security access information and configuration services;
   iii. comply with all applicable laws and regulations with respect to its activities under this Agreement;
   iv. carry out all other CLIENT responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the CLIENT's provision of such assistance as agreed by the parties, MERIDIAN may adjust any agreed timetable or delivery schedule as reasonably necessary;
   v. ensure that the Authorized Users use the Services and the Documentation in accordance with the terms and conditions of this Agreement and shall be responsible for any Authorized User's breach of this Agreement;

vi. obtain and maintain all necessary licenses, consents, and permissions necessary for MERIDIAN, its employees, subcontractors and/or agents to perform their obligations under this Agreement, including without limitation the Services;

vii. ensure that its network and systems comply with the relevant specifications provided by MERIDIAN from time to time; and

viii. be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to MERIDIAN'S data centers, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the CLIENT's network connections or telecommunications links or caused by the internet.

10. Indemnification

a. MERIDIAN and CLIENT agree to indemnify, defend and hold harmless the other, and their respective officers, directors, employees, partners and shareholders, from and against all claims, losses, demands, damages or costs, including attorneys' fees, arising from any source, including but not limited to the intentional or negligent acts, errors or omissions of the other or its officers, directors, employees, partners, and shareholders, or anyone for whom either MERIDIAN or CLIENT is legally liable, arising out of the performance of this Contract Agreement. MERIDIAN will have no obligation to defend CLIENT with respect to any claim, demand, action or proceeding, described herein, that is based upon (i) use of other than the then-current release of the Software, if infringement could have been avoided by use of the then-current release and the then-current release has been made available to CLIENT; (ii) use of the Services in conjunction with CLIENT's data, where use with such data gave rise to the infringement claim; (iii) use of the Services with other software, where use of such other software gave rise to the infringement claim; (iv) use of any Services in a manner inconsistent with its documentation; or (v) use of any Services in a manner that breaches this Contract Agreement. CLIENT will defend MERIDIAN from and against any and all liability, damage, loss or expense (including reasonable attorneys' fees) arising out of any claim, demand, action or proceeding based on allegations arising as a result of (i) use of the Services by CLIENT in conjunction with any data, equipment or software not provided by MERIDIAN, where the Services would not itself be infringing or otherwise the subject of the claim; (ii) use of the Services by CLIENT in a manner not permitted by this Agreement; (iii); (iv) use of the Services by CLIENT in any unlawful, improper or inappropriate manner or for any unlawful, improper or inappropriate purpose; (v) any claim of infringement of any patent or copyright or misappropriation of any trade secret in which CLIENT or any affiliate of CLIENT has a pecuniary or other material interest; or (vi) breach of any of CLIENT's warranties or covenants.

11. Term and Termination

a. The term of this Agreement will begin on the Effective Date and shall continue for the Initial Subscription Term and, thereafter, shall be automatically renewed for successive periods of twelve (12) months ("Renewal Period"), unless:
   i. Either party notifies the other party of termination, in writing, at least sixty (60) calendar days before the end of the Initial Subscription Term or any subsequent Renewal Period, in which case this Agreement shall terminate upon the expiration of the applicable Initial Subscription Term or Renewal Period; or
   ii. Otherwise terminated in accordance with the provisions of this Agreement; and the Initial Subscription Term together with any subsequent Renewal Periods shall constitute the entire Subscription Term.

b. Either party may terminate this Agreement immediately upon notice to the other party if such other party materially breaches a provision of this Agreement or Schedule, as applicable, and fails to cure such breach within thirty (30) calendar days after receipt of notice of such breach from the non-breaching party. If, in the sole judgment of the non-breaching party, such breach cannot reasonably be cured within such thirty (30) calendar day period, the non-breaching party may, in its sole discretion, grant the breaching party an additional thirty (30) calendar day period following the expiration of the first thirty (30) calendar day period in which to cure such breach; provided that the non-breaching party may terminate this Agreement or such Schedule, as applicable, immediately if the breaching party has failed to cure such breach within such second thirty (30) calendar day period.

c. Either party may terminate this Agreement immediately upon notice to the other party if such other party (i) files for or has filed against it a bankruptcy petition and such petition is not dismissed within sixty (60) calendar days after the filing date, (ii) becomes insolvent or (iii) makes an assignment for the benefit of its creditors.

12. Effect of Termination

a. Upon the expiration or termination of this Agreement,
   i. all rights granted to CLIENT under this Agreement will immediately terminate;
   ii. CLIENT will cease any further use of the Services.

b. At MERIDIAN'S request, CLIENT will verify in writing to MERIDIAN that CLIENT has taken the actions described in Section 12(a)(ii). MERIDIAN may destroy or otherwise dispose of any of the CLIENT Data in its possession unless MERIDIAN receives, no later than ten (10) business days after the effective date of the termination of this Agreement, a written request for the delivery to the CLIENT of the then most recent back-up of the CLIENT Data. MERIDIAN shall use reasonable commercial efforts to deliver the back-up to the CLIENT within thirty (30) calendar days of its receipt of such a written request, provided that the CLIENT has, at that time, paid all fees and charges outstanding at and resulting from termination (whether or not

due at the date of termination). The CLIENT shall pay all reasonable expenses incurred by MERIDIAN in returning or disposing of CLIENT Data. The accrued rights of the parties at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination shall not be affected or prejudiced. The rights and obligations of each of the parties set forth in Sections 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14, 17, 18, 20, 21, 23, 24 and 25 and any other Section or Statement herein that by its nature is intended to survive will survive the expiration or termination of this Agreement. Any payments owed by CLIENT as of the termination date shall become immediately due and payable.

13. Limitation of Liability

a. EXCEPT IN THE CASE OF AN INFRINGEMENT BY CLIENT OF ANY OF MERIDIAN'S PROPRIETARY RIGHTS, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY LOST PROFITS, LOST DATA OR SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY NATURE, FOR ANY REASON, INCLUDING, WITHOUT LIMITATION, THE BREACH OF THIS AGREEMENT OR ANY TERMINATION OF THIS AGREEMENT, WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY) OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN WARNED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OF ANY KIND. EXCEPT AS EXPRESSLY SET FORTH HEREIN, ALL REMEDIES, INCLUDING, WITHOUT LIMITATION, THE TERMINATION OF THIS AGREEMENT AND ALL OF THE REMEDIES PROVIDED BY LAW (AND NOT EXCLUDED PURSUANT TO THE FOREGOING SENTENCE) WILL BE DEEMED CUMULATIVE AND NOT EXCLUSIVE. IN NO EVENT WILL THE LIABILITY OF MERIDIAN UNDER THIS AGREEMENT EXCEED THE TOTAL FEES PAID BY CLIENT HEREUNDER DURING THE TWELVE (12) MONTHS PRIOR TO THE DATE ANY CLAIM IS MADE AGAINST MERIDIAN.

14. Government Use/Procurement

a. MERIDIAN provides the Service and access to the Software for ultimate U.S. Government end use solely in accordance with the following: Government technical data and software rights related to the Service and the Software include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a need for rights not conveyed under these terms, it must negotiate with MERIDIAN to determine if there are acceptable terms for

transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable agreement.

b. Each party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Service and the Software. Without limiting the foregoing: (a) each party represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports; and (b) each Party shall not permit any User to access or use the Service and the Software in violation of any U.S. export embargo, prohibition or restriction.

15. Assignment

a. CLIENT may not assign or otherwise transfer this Agreement or its rights and obligations hereunder without the prior written consent of MERIDIAN, which consent will not be unreasonably withheld. Any transaction or series of transactions in which (i) more than fifty percent (50%) of the outstanding voting stock or membership interests of CLIENT are transferred to a third party, or (ii) all or substantially all of CLIENT's assets are sold to a third party, will be deemed an assignment of this Agreement. Any purported assignment or other transfer without the consent of MERIDIAN (a) will be void and of no force or effect, and (b) will constitute a material breach of this Agreement.

16. Force Majeure

a. Except for a party's payment obligations hereunder, neither party will be deemed in default of this Agreement to the extent that performance of its obligations, or attempts to cure any breach thereof, are delayed or prevented by reason of any act of God, fire, natural disaster, accident, terrorist attack, act of government, network or telecommunication system failure, sabotage or any other cause beyond the control of such party ("Force Majeure"), provided that such party promptly gives the other party notice thereof. In the event of such Force Majeure, the time for performance or cure will be extended for a period equal to the duration of the Force Majeure but not in excess of six (6) months.

17. Severability

a. If a court of competent jurisdiction determines that any provision of this Agreement is illegal, invalid or otherwise unenforceable for any reason, such provision will be deemed stricken to the extent that it is illegal, invalid or otherwise unenforceable. All remaining provisions will remain in full force and effect and this Agreement will be interpreted as if it had not contained the severed provision.

18. Governing Law

a. Issues regarding the validity, ownership or enforcement of any copyright, patent, trademark or other proprietary right licensed or sublicensed hereunder will be determined under the applicable law of the United States and the Commonwealth of Virginia, as applicable. With

respect to all other issues, this Agreement will be construed under and governed by the substantive laws of the Commonwealth of Virginia without resort to conflict of laws principles. Each party agrees that any legal proceeding commenced by one party against the other party under this Agreement will be brought in any state or Federal court having jurisdiction over Fairfax County, Virginia. Each party submits to such jurisdiction and waives any objection to venue or claim of inconvenient forum. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

19. Headings

a. Captions and section headings used herein are for reference purposes only and will not control or alter the meaning of this Agreement as set forth in the text.

20. Waiver

a. A waiver of any right under this Agreement is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

b. Unless specifically provided otherwise, rights arising under this agreement are cumulative and do not exclude rights provided by law.

21. Notices

Any notice required to be given under this agreement shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other party at its address set out in this agreement, or such other address as may have been notified by that party for such purposes. A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 AM on the first business day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post.

If to MERIDIAN:	With a copy to:	If to CLIENT: ATTN:
ATTN: Contracts Meridian Knowledge Solutions, LLC 2001 Edmund Halley Dr. Suite 400 Reston, VA 20191	ATTN: Legal Department Meridian Knowledge Solutions, LLC 80 Iron Point Circle, Suite 100 Folsom, CA 95630	<CLIENT_ATTENTION_LEGAL> <CLIENT_LEGAL_ADDRESS_1> <CLIENT_LEGAL_ADDRESS_2> <CLIENT_LEGAL_CITY_STATE_ZIP>

22. No Partnership or Joint Venture

a. Nothing in this agreement is intended to or shall operate to create a partnership between the parties, or authorize either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power). This Agreement shall not prevent MERIDIAN from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation, products and/or services which are similar to those provided under this Agreement.

23. Non-Solicitation

a. In addition to the obligations set forth in Section 5, during the term of this Agreement and for a period of twelve (12) months immediately following the last occurrence of any introductions, interviews, or provision of services under this Agreement, CLIENT agrees not to solicit or hire, indirectly or directly, in either an employee or independent contractor capacity, any individual who (i) was introduced under this Agreement; (ii) the CLIENT has interviewed under this Agreement; (iii) has provided services under this Agreement, or (iv) the CLIENT or its employees, representatives and or agents have received information about or as the result of any introduction, interview or service provided under this Agreement. Should the CLIENT breach this Section of the Agreement in any instance the CLIENT will pay MERIDIAN an amount of two (2) times the then current annual salary (including any applicable bonus compensation) of the individual solicited directly to MERIDIAN. Said payment will be made within fifteen (15) calendar days of the breach as notified in writing by MERIDIAN to the CLIENT. The Parties hereto further agree that the limit on liability as defined herein does not apply to this Section 23.

24. Disputes and Arbitration

a. The parties agree that in the event of a dispute or alleged breach they will work together in good faith to resolve the matter internally by escalating it to higher levels of management and, if necessary, to use a mutually agreed upon alternative dispute resolution mechanism (other than arbitration) prior to resorting to arbitration. If the parties are unsuccessful at resolving said dispute or alleged breach, then the parties shall seek arbitration. Except as set forth in Section 5, the parties agree to submit to binding arbitration within six (6) months of the last event giving rise to any controversy arising out of this Agreement or involving the construction or application of any of the terms of this Agreement and to waive any statute of limitations to the contrary. Notification to the other party of a written request for arbitration shall comply with Section 22 governing Notices. Any timely and properly noticed request for arbitration shall be submitted to binding arbitration through the American Arbitration Association pursuant to its Commercial Arbitration Rules. Each party shall pay for its own attorneys' fees and costs for the arbitration. The parties shall split equally the cost of the arbitrator. Both parties are entitled

to conduct discovery in accordance with any applicable law. The arbitrator shall apply Virginia and Federal law to the issues presented and shall issue a written memorandum of decision. The decision of the arbitrator shall be final and binding, and the parties waive the right to a jury trial, a trial de novo or appeal except for the purpose of enforcing the arbitrator's decision. The prevailing party will be entitled to recover reasonable attorneys' fees and costs of any action for enforcement, the amount of any such attorneys' fees and costs award to be determined by the Arbitrator.

b. Except as set forth in Section 5 with regard to injunctive relief, the parties expressly state that it is their intent to arbitrate disputes between them. Therefore, this Agreement shall be construed so as to be consistent with applicable Federal and Virginia law and to be enforceable to the maximum extent allowable by law to provide arbitration as the forum to resolve their disputes. If necessary, any portion of this Agreement that is unenforceable by law shall be stricken, and the arbitrator or the court, as the case may be, shall have the power to reform this Agreement to the extent necessary to comply with applicable law and to give effect to the parties' intent that they shall arbitrate their disputes.

25. Publicity

CLIENT grants MERIDIAN permission to utilize the CLIENT's trademarks, trade names, or other designations in any promotion, press release or publication.

26. Entire Agreement

a. Except as otherwise provided for herein, this Agreement constitutes the entire agreement between the parties pertaining to the subject matter hereof and supersedes all prior and contemporaneous agreements, negotiations and understandings, oral or written, between the parties with respect to the subject matter hereof. This Agreement will be binding on and inure to the benefit of the legal representatives, successors and permitted assigns of the parties. This Agreement may not be modified or refined unless amended by both Parties under a written and signed amendment. The issuance of any additional terms and conditions by either Party hereto included with purchase orders or other documents are null and void. In the event of any conflict between these General Terms and Conditions and a provision of any Schedule, the provision of the Schedule will control, but only with respect to the subject matter of the Schedule.

27. Subscription Term and Fees

a. **Software.** Meridian LMS Learning Management System

b. **Modules/Components**. The following additional modules and components are included/enabled:

i. None

c. **Languages**. The following language packs are included/enabled:
i. English (US) [included]

d. **Initial Subscription Term**
The initial term of this subscription will be <SUBSCRIPTION_TERM> commencing from the Effective Date of this Agreement.

e. **Renewal Period Terms**
Upon expiration of the Initial Subscription Term, this Agreement will be renewable in subsequent <SUBSCRIPTION_RENEWAL_TERM> terms based on the then current pricing for the Applications, Modules/Components, and Languages listed above.

f. **Number of Authorized Users. Maximum of <AUTHORIZE_USERS_> active users**
"Authorized users" is defined as the total number of user accounts that have accessed the system during the annual subscription term.

g. **Additional User Subscription Fees**
Additional "Authorized Users" can be added at any time during the Initial Term or Renewal Period Terms based on the then current Subscription pricing for additional users.

h. **Bandwidth and Storage**
The following bandwidth and storage limitations are included as part of this Agreement. Any additional bandwidth or storage required by CLIENT will be subject to current published price list.

- Bandwidth: 100GB/month (1.2 TB/annually – measured annually)
- Additional content storage is priced at $500 annually for 100 GB.

Bandwidth will be measured based upon total in/out traffic. Bandwidth will be monitored on a monthly basis in relation to the commitments levels, however bandwidth will be measured based upon total usage over the annual term. Overage fees may apply go consuming more bandwidth.

i. **Subscription Fees**
i. The following subscription fees apply to this Agreement: <SUBSCRIPTION_FEES> per year during the Initial Subscription Term.

j. **Set-up Fee**
i. The following set up fees apply to this Agreement, and are defined in Schedule One (1) of this agreement: <SETUP_FEES>

k. **Optional Services/Module Fees**
   i. The following optional modules and services are available. The respective fees are included in Schedule One (1) of this agreement.
   <OPTIONAL_MODULES_SERVICE_FEES>

j. **Optional Historical Data Migration:**
   i. The respective scope of Services to be provided are defined in Schedule One (1) below.
   <OPTIONAL_DATA MIGRATION_SERVICE_FEES>

28. Service Level Agreements: **Software Support, Software Availability and Maintenance**

The Services provided by MERIDIAN under this agreement are bound by the Service Level Agreement (SLA) as described herein. In the case of an SLA violation, the respective remedies described herein will apply. The SLA penalty applicable in any given month is subject to a total cumulative penalty cap of 10% of the current month's hosting service fees ("Service Credits"). Any Service Credits due under this agreement will be credited promptly but in no event later than the quarter following the calculation of the Service Credit.

MERIDIAN will be provided a ramp up period of ninety (90) days from software Go Live (Production go live date) before any SLA requirements and subsequent remedies go into effect.

System Availability: will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time (measured in minutes) during such month, and thereafter dividing the difference so obtained by the total time during such month. Represented algebraically, System Availability for any particular calendar month is determined as follows:

$$\text{System Availability} = \frac{\text{(Total Monthly Time – Unscheduled Downtime)}}{\text{Total Monthly Time}}$$

Note: "Total Monthly Time" is deemed to include all minutes in the relevant calendar month excluding minutes of downtime caused by Scheduled Downtime, only to the extent such minutes are included within the Subscription Agreement Term.
MERIDIAN will undertake commercially reasonable measures to ensure that System Availability equals or exceeds 99.70 % during each calendar month.

a. **Measurement and Reports:** MERIDIAN will monitor System Availability metrics on an ongoing basis. All measurements of System Availability will be calculated on a monthly basis for each calendar month during the term of this agreement. MERIDIAN shall provide the System Availability report to CLIENT, on an as required basis, when requested by CLIENT.

This report will contain performance metrics against the System Availability SLA obligations as depicted herein; and specific to unscheduled downtime events only.

b. **Remedies:** In the event System Availability is not equal to or greater than 99.70% for a given month, CLIENT will be entitled to service level credits against its subsequent payment obligations (as set forth in this Subscription Agreement) according to the following:

System Availability	Available Credit *(% of monthly service fee)*
99.70% - 100.00%	No Credit.
95.00% - 99.69%	Three percent (3%) of the applicable monthly hosted service fees for the applicable calendar month.
90.00% - 94.99%	Six percent (6%) of the applicable monthly hosted service fees for the applicable calendar month.
<89.99%	Ten percent (10%) of the applicable monthly hosted service fees for the applicable calendar month.

CLIENT's credits under this section are CLIENT's sole and exclusive remedy with respect to any Unscheduled Downtime or any failure by MERIDIAN to meet the Service Availability required by this agreement. The monthly available credit is capped at the lesser of $5,000 or the total cap as set forth in the System Availability section herein.

MERIDIAN will exercise commercially reasonable efforts to initiate remedial activity within two (2) hours of CLIENT reporting the unscheduled downtime to MERIDIAN.

c. **Exceptions**
CLIENT shall not receive any credits in connection with any failure or deficiency Availability caused by or associated with:

i. Force Majeure events beyond MERIDIAN's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, armed conflict, embargo, fire, flood, strike or other labor disturbance, interruption of or delay in transportation, unavailability of or interruption or delay in telecommunications or third party services, virus attacks or hackers, failure of third party software (including, without limitation, ecommerce software, payment gateways, chat, statistics or free scripts) or inability to obtain raw materials, supplies, or power used in or equipment needed for provision of this Schedule;
ii. Failure of access circuits to the ISP Network, unless such failure is caused solely by MERIDIAN;
iii. Scheduled maintenance and emergency maintenance and upgrades;
iv. DNS issues outside the direct control of MERIDIAN;
v. Issues with FTP, POP, or SMTP CLIENT access;

vi. False Schedule breaches reported as a result of outages or errors of any MERIDIAN measurement system;
vii. CLIENT's acts or omissions (or acts or omissions of others engaged or authorized by CLIENT), including, without limitation, custom scripting or coding (e.g., CGI, Perl, HTML, ASP), any negligence, willful misconduct, or use of the Services in breach of MERIDIAN's Terms and Conditions and Acceptable Use Policy;
viii. E-mail or webmail delivery and transmission;
ix. DNS (Domain Name Server) Propagation; and / or
x. Outages elsewhere on the Internet that hinder access to your account. MERIDIAN is not responsible for browser or DNS caching that may make your site appear inaccessible when others can still access it. MERIDIAN will guarantee only those areas considered under the control of MERIDIAN: MERIDIAN server links to the Internet, MERIDIAN'S routers, and MERIDIAN'S servers.

d. **Software Support**

MERIDIAN will apply service packs, improvements, and enhancements as they are released to the Subscription platform. MERIDIAN will provide CLIENT with access to the Customer So

i. Up to five (5) named system administrators will receive access the CCC and MERIDIAN's web-based customer support portal.
ii. Notification of and access to Updates in base product format that MERIDIAN makes generally available to its Clients who have paid a maintenance support fee. Modifications to base format Updates as a result of CLIENT specific enhancements and integrations or installation support of Updates is not included as part of Standard Maintenance. Upon receipt of an Update by CLIENT, such Update will be deemed to be part of the Software for all purposes of the License Agreement.
iii. Help desk support and guidance on the use of existing base product functions. Effort exceeding a total of one (1) hour per one function is considered Training and is not included as part of Standard Maintenance Support.
iv. Troubleshooting issues associated with base product functions. If a base bug is identified, the CCC will report it to the Meridian Product team. If the issue falls within the scope of the Limited Warranty set forth in the Software License Agreement, the terms of the Limited Warranty shall apply. Base bug resolution is managed by the Meridian Product team. Determination of the need and prioritization of Updates to address reported issues outside of the scope of the Limited Warranty is at the sole discretion of MERIDIAN, and this Exhibit C-1 shall not be construed as an addition or change to the terms set forth in the Limited Warranty of the Agreement.
v. CCC Support Hours can be provided during standard business hours or 24/7. CLIENT support hours are as defined in the table below:

CCC Support Hours (Selection Marked with "X")

X	Standard	Standard business days only, from 8am to 8pm Eastern Time by telephone and/or Meridian support portal
	Extended	24/7 access by telephone or Meridian support portal

The Client acknowledges from time to time in Company's sole discretion but using commercially reasonable efforts to minimize any disruption of the Service, MERIDIAN will schedule standard system maintenance, including version upgrades to the Software and/or system, in which case MERIDIAN will announce the scheduled maintenance via e-mail to CLIENT's designated e-mail address.

e. **Software Support Severity Level Definitions**

All reported issues to the CCC will be assigned a Severity Level which defines the critical nature of the problem. The Severity Level will drive CCC response to the CLIENT, internal escalation process, on procedures per a defined timeline.

The following table defines the four (4) standard Severity Levels that will be assigned to MERIDIAN documented issues. Subsequent tables outline the notification and escalation processes for each defined Severity Level.

Severity Level	Severity Description	Response Time
1 Critical	Issue that causes complete loss of service to the CLIENT's production environment and work cannot reasonably continue. Workarounds to provide the same functionality are not possible and cannot be found in time to minimize the impact on the CLIENT's business. The problem has one or more of the following characteristics: Fifty percent of users cannot access the system. Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, loss of functionality that is financially impacting. Severe performance degradation rendering the system unusable. Loss of data that cannot be reasonably retrieved. Security vulnerabilities that could expose PII data.	One (1) Hour

2 Major	Issue where operation of the system is considered severely limited, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics: A software error for which there is a Customer acceptable workaround. Self-contained issue that does not impact the overall functionality of the software. Minimal performance degradation which impacts productivity.	One (1) business day
3 Minor	Issue that causes no loss of service and in no way impedes use of the system. The problem has one or more of the following characteristics: Guidance on the use of existing base product functions and Customer accepted modifications. Cosmetic issue such as misspelled words or misaligned text. Enhancement requests to update functionality.	Two (2) business days
4 Minimal	Questions regarding system functionality where product user guides are confusing or non- existent and answers are limited to under thirty (30) minutes.	Three (3) business days

CLIENT Responsibilities: To provide effective support, additional information may be required by CLIENT. Additional details regarding MERIDIAN and CLIENT responsibilities are documented in the MERIDIAN Customer Support Policy.

f. Support Exclusions.
The following services are not included Support, but can be provided as separate, optional tasks:

i. Training on Software functions and modifications in excess of standard help desk support. Training shall be defined as one or more discussions about one function within the Software, where the total discussion time exceeds one (1) hour.
ii. End User support, or support to any person other than the five named administrators.
iii. Troubleshooting or resolution of hardware, software, security, or network-related issues on CLIENT servers or workstations.
iv. Project management support, including administration of CLIENT funding and project reports to CLIENT.
v. Courseware support, including loading of content into the site, troubleshooting issues with third party or client developed courseware, or troubleshooting user or browser configuration or related issues with viewing courseware.
vi. Integration with CLIENT applications (such as Active Directory, HRIS, or others).

g. **Credit Request and Payment Procedures.**
In order to receive a credit for system availability as defined in Section 28b herein, CLIENT must make a request therefore by sending an email message to creditrequest@meridianks.com. Each request in connection with this Schedule must include CLIENT's account number (per MERIDIAN's invoice) and the dates and times of the unavailability of CLIENT's Web site and must be received by MERIDIAN within ten (10) business days after CLIENT's Web Site was not available. If the unavailability is confirmed by MERIDIAN, credits will be applied within one week after MERIDIAN's receipt of CLIENT's credit request.

Notwithstanding anything to the contrary herein, the total amount credited to CLIENT in a particular month under this Service Level Agreement shall not exceed the total Subscription fee paid by CLIENT for such month for the affected Services. Credits are exclusive of any applicable taxes charged to CLIENT or collected by MERIDIAN and are CLIENT's sole and exclusive remedy with respect to any failure or deficiency in the Availability of Service.

29. Survival
In the event of any termination of the Agreement, Sections 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 27, 28, and 29 shall survive and continue in effect.

MERIDIAN:	CLIENT:
MERIDIAN KNOWLEDGE SOLUTIONS, LLC, a Virginia, limited liability company	
By:	By:
Printed Name:	Printed Name:
Title:	Title:
Date:_____	Date: _____

SCHEDULE 1
IMPLEMENTATION SERVICES SET UP AND OPTIONAL SERVICES
STATEMENT OF WORK # SOW-001

This Schedule One (1) Statement of Work ("SOW") defines the implementation Services being provided by MERIDIAN to CLIENT under the terms and conditions of the Software as a Service and Subscription Agreement; in order to enable MERIDIAN to deliver and CLIENT to receive those Software Services; and is executed by and between MERIDIAN and CLIENT.

A. Summary of Scope Implementation Professional Services

1. Standard Deliverable Summary

Meridian LMS software will be delivered to CLIENT preconfigured with standard settings derived from best practices. CLIENT will be provided a limited set of software configurable options that can be personalized to enable the software to meet their business needs (i.e. SCORM settings, Virtual meeting setup, domain configurations). MERIDIAN will (1) work with CLIENT to determine how these options should be configured and (2) implement each option based on the set of configurable parameters inherent to the software. Configuration will be limited to the product capabilities outlined in the current version of the MERIDIAN manuals and documentation as well as the scope defined herein.

The following table summarizes the software setup tasks that MERIDIAN will provide on a <SOW_FFP_OR_T&M> basis. Details and scope of these services are further defined in Section B herein.

Standard Software Setup Tasks	
1. Installation of Meridian LMS Environments	**2.** Discovery Session/Joint Requirements Development (JRD)
3. Configuration & Branding Application	**4.** System Integration
5. Production Installation	**6.** Training
7. Go Live Support	
Optional S	
8. Historical Data Migration	**9.** Single Sign-On
10. E-Commerce Integration	**11.** Meridian Social
12. Meridian Mobile	**13.** AdHoc
14. Additional Training	

2. Change Control

CLIENT acknowledges and agrees that a fundamental guiding principle for planning and executing this process, including the establishment of the User requirements, will be the utilization of existing functionality of the Meridian LMS application on an out of the box basis. This functionality will be used to implement and deploy the requirements as defined herein and further by the Requirements documentation to be mutually developed and approved with the CLIENT. The estimated consulting fees and the planned schedule are based on this principle. The purpose of the Change Management process is to ensure that requests for Project changes (to requirements or software configuration) are properly recorded, evaluated/assessed, properly dispositioned, and incorporated into the software implementation scope as required, and schedules with the proper priority and deliverable due dates.

B. Scope Details

MERIDIAN will setup CLIENT's solution according to the following in-scope details. Each task is documented below, along with the MERIDIAN and CLIENT deliverables associated with each task, assumptions, and the acceptance criteria.

Any additional configurations, or e-learning consulting by MERIDIAN, outside the scope defined herein, can be performed by:

a. MERIDIAN Professional Services on a fixed fee or time and materials basis under a separate change request, or
b. CLIENT upon the completion of MERIDIAN Administration training.

MERIDIAN offers its Direct Labor Rates as depicted herein. Cost estimates for any additional services will be provided to CLIENT upon CLIENT'S request. Upon execution of the Schedule 2 Change Order, defining the additional work to be performed, associated cost and any other relevant information, MERIDIAN will commence work.

1. Standard Setup Tasks: Installation of Meridian LMS Environments.

The purpose of this task is to establish the Meridian LMS pre-production environments that support the software implementation lifecycle as outlined further in this SOW and ensure configuration management between software environments.

The following software environments will be installed with out of the box settings as part of this task.

Meridian LMS Environments	
Stage (External)	MERIDIAN'S Staging Environment is an environment that is utilized to setup the CLIENT software based upon scope defined herein. The Stage environment is available for CLIENT Acceptance Testing, allowing project participants and stakeholders to log in and review overall functionality,

	implementation configurations, product extensions, and integrations that are applicable.

MERIDIAN Deliverables	CLIENT Deliverables
• Establish Stage environment described as aforementioned under section 1. • Provide Client project manager URL, login, and password to stage environment. • Provide system baseline documentation.	• Confirmation of receipt of URL and access to the stage environment.
Assumptions	**Acceptance Criteria**
• Additional pre-production environments are not included in this effort. • CLIENT will report access within three (3) days of receiving the access information.	• Client receipt of stage environment credentials and confirmed access. • Receipt of baseline documentation.

2. Standard Setup Tasks: Discovery Session/Joint Requirements Development (JRD)

The purpose of this task is for the facilitation of the Discovery/Joint Requirements Development Session to establish Meridian LMS application branding, system configurations, and integrations. Furthermore, this session provides high level business process mapping to the Meridian LMS application.

MERIDIAN Deliverables	CLIENT Deliverables
• Deliver one (1) day virtual session • Provide software application branding checklist. • Document configuration requirements in the Meridian Standard Requirements Document. • Rough Order of Magnitudes (ROMs) related to any scope changes or new tasks identified.	• Provide proper resources as depicted herein. • List of attendees, coordinate date/times, location(s), and meeting equipment needs. • Participate in follow up conference calls to complete the Requirements Documentation.
Assumptions	**Acceptance Criteria**
• One (1) day virtual. • Use Case and Functional Requirements associated to specific integrations are not in scope.	• System configuration requirements are complete and documented. • Delivery of session.

3. Standard Setup Tasks: Configuration and Branding Application

The purpose of this task is to configure and test the Meridian LMS software application based upon the completed and approved Requirements Document as defined in task B.2 above.

MERIDIAN Deliverables	CLIENT Deliverables
• Complete the setup of all agreed upon software application configurations. • Setup One (1) branded Meridian LMS CLIENT specific skin.	• Graphics per branding checklist specifications.
Assumptions	**Acceptance Criteria**
• Application Branding – MERIDIAN will deliver one (1) round of final pre-production skin mock up to the CLIENT for review and approval prior to setup in the Meridian LMS CLIENT Stage environment. • Application Branding – MERIDIAN will deliver one (1) round of final pre-production skin review and changes upon applying to the Meridian LMS CLIENT Stage environment. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	• Configurations completed and tested per the Requirements specified in task B.2 above. • Meridian LMS application CLIENT Branded skin configured and tested, per the Requirements specified in task B.2 above.

4. Standard Setup Tasks: System Integration

The purpose of the following task is to setup the inbound to Meridian LMS HRIS Integration. The HRIS inbound feed transmits employee detail from CLIENT's HR system to MERIDIAN (e.g. Employee Name, Organization, and Job Title).

CLIENT will provide three (3) flat files to MERIDIAN, in MERIDIAN's format, for the inbound processing and loading of HRIS data (Organizations, Job Titles, User data). The HRIS/DAILY FEED data (flat files) must follow the specifications designated in MERIDIAN's HRIS templates. Any extension of the file schema's and/or processing/validation requirements may result in an expansion of scope for this task and may require additional funding. Meridian's tool to process the aforementioned flat files performs the appropriate inserts and updates of Organization Data, Job Titles, then Users, processing all data through the native API's of Meridian LMS.

MERIDIAN Deliverables	CLIENT Deliverables

• MERIDIAN Base HRIS template. • Configuration of the Meridian LMS HRIS Tool based upon the completed Requirements Document specified in task B.2 above. • One pre-production load of a subset of CLIENT production ready data for CAT purposes. • One production load of full user data into the CLIENT production environment.	• Backfill and delivery of the three (3) flat files to Meridian for processing: User Data, Organizations, Job Titles.
Assumptions	**Acceptance Criteria**
• One way HRIS integration inbound to the Meridian LMS application only. • Meridian configure the HRIS and load a subset of CLIENT production ready user data in the Meridian LMS CLIENT Stage environment for testing purposes. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein. • Upon completion of CAT, MERIDIAN will load a full set of CLIENT production data in the Meridian LMS CLIENT production environment.	• HRIS Tool configured and tested per the Requirements specified in task B.2 above, in the Meridian LMS CLIENT Stage environment. • One (1) final data load in Meridian LMS CLIENT Production environment.

5. Standard Setup Tasks: Production Installation

The purpose of this task is to complete the installation of the Meridian LMS base application, database, configurations, branding and integrations into the Meridian LMS CLIENT production environment.

MERIDIAN Deliverables	CLIENT Deliverables
• Meridian LMS CLIENT production base code and database installation. • MERDIAN will apply applicable configurations, branding, and integrations.	• Validation Meridian LMS CLIENT Production install is completed per the Requirements specified in task B.2 above.
Assumptions	**Acceptance Criteria**
• Limited to the installation of the application and database of one instance of the Meridian LMS CLIENT production environment.	• Meridian LMS CLIENT Production application has been installed and is accessible per the Requirements specified in task B.2 above.

• Technical support does not extend to other software or hardware support, data integration/migration or the resolution of base product issues. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	

6. Standard Setup Tasks: Training

The purpose of this task is to provide Implementation Readiness and Administrative training during the project implementation. The description of these trainings and the number of respective days is provided below.

Training Types Definitions

- o Implementation Readiness Training (IRT) – two (2) days – The purpose of IRT is to level set terminology and provide core system concepts and features as it relates to key decisions that will be required during the Discovery/Joint Requirements Development Session.
- o Administrative – two (2) days – The purpose of Administrative training is to provide the in-depth knowledge necessary to support administration system features and functions for the set up and management of the Meridian Learning Management System.

MERIDIAN Deliverables	CLIENT Deliverables
• Conduct required training sessions as depicted herein. • Printed Student Guides for up to twelve (12) people.	• Provide list of trainees, location(s), and training equipment in order to facilitate a hands-on training and demonstration of product features and functionality. • Pre-approval of travel reimbursement, if onsite instructor led training is required.
Assumptions	**Acceptance Criteria**
• No more than twelve (12) people. • Travel costs are not included in the cost. • Implementation Readiness Training is provided prior to the Discovery/Joint Requirements Session. • Administrative Training is typically provided towards the end of the implementation.	• Delivery of the scoped number of days of training by type.

schedule, prior to the Customer Acceptance Testing initiation; but can be mutually agreed upon. • A minimum of two (2) weeks' notice is required prior to the scheduling of training in order to appropriately manage resource schedules and minimize travel costs/impacts. • End User Training is not provided within the current scope of services. • Train-the-Trainer Training is not provided within the current scope of services. • Technical Training is not provided within the current scope of services.	

Training Cancellation Policies

Rescheduling or cancellations may result in a cancellation fee per the following schedule, plus any reasonable and necessary expenses incurred as a result of preparing to deliver the training described herein. Notification of a cancellation or reschedule must be made to MERIDIAN in writing.

- More than 20 business days prior to training – 0% of standard Training fee.
- 11-20 business days prior to training start – 25% of standard Training fee.
- 6-10 business days prior to training start – 50% of standard Training fee.
- 0-5 business days prior to training start – 100% of standard Training fee.

7. Standard Setup Tasks: Go-live Support

The purpose of this task is to provide CLIENT support from the initial deployment of configurations, branding, and integrations into the Meridian LMS CLIENT Production environment. This period allows the CLIENT to validate that Meridian LMS application containing all configuration, and integrations into the Production environment. Furthermore, it is the period in which the CLIENT is to finalize administrative configuration settings, new course and content readiness.

MERIDIAN Deliverables	CLIENT Deliverables
• Delivery of final branding, configurations, and integrations into the Meridian LMS CLIENT Production environment.	• Final sign-off on the delivery of the respective deliverables as stated in task B herein, by MERIDIAN.
Assumptions	**Acceptance Criteria**

• Go live support consist of ten (10) business days' worth of implementation resource support post completion of the initial deployment into the Meridian LMS CLIENT Production environment. • Extension of the Go Live task as defined herein will require additional funding.	• Completion of ten (10) business day's duration beyond the completion of the initial deployment into the Meridian LMS CLIENT Production environment.

8. Optional Setup Tasks: Historical Data Migration

The purpose of this task is to provide a Data Migration with the standard Meridian LMS implementation services as depicted herein. The Legacy Data Migration (migration of user historical transcript data to Meridian LMS), Meridian will support a one-way, inbound, one-time Production data migration to import historical data based on the maximum record set of up to 100,000 records.

MERIDIAN Deliverables	CLIENT Deliverables
• MERIDIAN Base Data Migration template. • Configuration of the Meridian LMS HRIS Tool based upon the completed Requirements Document specified in task B.2 above. • One pre-production load of a subset of CLIENT production ready data for CAT purposes. • One production load of full user data into the CLIENT production environment.	• Backfill and delivery of the one (1) flat file to Meridian for processing: User Data, Transcripts.
Assumptions	**Acceptance Criteria**
• One-way inbound Data Migration into the Meridian LMS application only. • CLIENT cannot change the format of the Data Migration XLS file template. • Meridian will load a subset of CLIENT production ready historical data in the Meridian LMS CLIENT Stage environment for testing purposes. • Content is not included in-scope. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	• Data Migration completed and tested per the Requirements specified in task B.2 above, in the Meridian LMS CLIENT Stage environment. • One (1) final data load in Meridian LMS CLIENT Production environment.

MERIDIAN Deliverables	CLIENT Deliverables
• Upon completion of CAT, MERIDIAN will perform a one-time full data load of CLIENT production data in the Meridian LMS CLIENT production environment.	

9. Optional Setup Tasks: Single Sign-On

The purpose of this task is to provide an Active Directory or SAML integration with the Meridian LMS implementation. Setup is limited to the Meridian LMS application out-of-the-box solution for the integration of Microsoft Active Directory services/LDAP/SAML 2.0.

MERIDIAN Deliverables	CLIENT Deliverables
• If Active Directory or LDAP: • Map Active Directory (AD) accounts to Meridian LMS using “sAMAccountName” or other unique identifier. • Establish service to query AD. • Configure IPsec tunnel. • If SAML 2.0: • Configure SAML Assertion Authentication. • Configure digital certificate for SAML signature validation. • Configure SSL certificate for Meridian LMS site.	• If Active Directory or LDAP: • Provide remote access and credentials to access AD/LDAP for application Business Logic to query for authentication. • Validate AD access in Meridian LMS CLIENT Stage and Production environment. • SAML 2.0: • Provide SAML Authentication environment. • Provide digital certificate to enable SAML digital signature on Meridian LMS hosting server. • Provide SSL certificate to enable secured communication between Meridian LMS and Authentication provider. • Validate SAML access in Meridian LMS CLIENT Stage and Production environment.
Assumptions	**Acceptance Criteria**
• Alternate or multiple Directory Services are out of scope. • Single Sign-On mechanism must be utilized/enforced across all domains. • SAML 2.0 Assertion integration assumes user accounts already exist in Meridian LMS	• AD/LDAP/SAML integration/access validated in Meridian LMS CLIENT Stage and Production environments; and per the Requirements specified in task B.2 herein.

and UID attributes of SAML assertion properly maps to the Meridian LMS Login ID. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	

10. Optional Setup Tasks: eCommerce Integration

The purpose of this task is to provide E-Commerce integration with the Meridian LMS implementation. The Meridian LMS application has native and standard integration capabilities with CyberSource's e-commerce engine. Meridian will support the configuration and setup of this integration (CyberSource solution) to work with Client's respective merchant account.

MERIDIAN Deliverables	CLIENT Deliverables
• Configuration of the Meridian LMS application e-Commerce functionality with Client's CyberSource account (one (1) Payment Gateway only).	• Provide MERIDIAN with the applicable Merchant Account credentials. (CyberSource).
Assumptions	**Acceptance Criteria**
• CLIENT will provide MERIDIAN with the Merchant Account credentials to support the required configurations of the Merchant Account to be used/integrated with the Meridian LMS application's e-commerce functionality. • Limited to one (1) payment Gateway only: Cybersource. • Any other Payment vendors requiring integration are not covered under this scope of work. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	• CLIENT validation of a successful transaction of purchase through e-commerce functionality into the live Merchant account. • Confirmation that the e-commerce functionality has been correctly configured and is functioning with Customer's account information, and in the Requirements specified in task B.2 herein.

11. Optional Setup Tasks: Meridian Social

The purpose of this task is to install and setup the standard Meridian Social module for the CLIENT. Setup is limited to the Meridian LMS out of the box solution for the Meridian Social module that includes supported features of the 3rd party integration.

MERIDIAN Deliverables	CLIENT Deliverables
• Configuration of the Meridian LMS application.	• Provide MERIDIAN confirmation of functionality is configured within Stage/Production environments.
Assumptions	**Acceptance Criteria**
• Functionality setup is limited to the base solution. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	• CLIENT validation of the access of the Social functionality via Meridian LMS user interface. • Confirmation that the Meridian Social functionality has been correctly configured and is functioning per the Requirements specified in task B.2 herein.

12. Optional Setup Tasks: Meridian Mobile

The purpose of this task is to install and setup the standard Meridian Mobile module for the CLIENT. Setup is limited to the Meridian LMS out of the box solution for the Mobile module that includes one branded application.

MERIDIAN Deliverables	CLIENT Deliverables
• Configuration of the Meridian LMS application. • One Branded Application.	• Provide MERIDIAN with the applicable iTunes and Google accounts for the application to be published. • Provide MERIDIAN confirmation of functionality is configured within Stage/Production environments.
Assumptions	**Acceptance Criteria**
• CLIENT to provide credentials for iTunes and Google to upload the application. If client desires to publish the application, this is recommended. • Functionality setup is limited to the base solution. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	• Confirmation that the Meridian Mobile functionality has been correctly configured and is functioning per the Requirements specified in task B.2 herein.

13. Optional Setup Tasks: AdHoc

The purpose of this task is to install and setup the standard AdHoc reporting module for the CLIENT. Setup is limited to the Meridian LMS out of the box solution for AdHoc module that includes identified base product views and data object relationships.

MERIDIAN Deliverables	CLIENT Deliverables
• Configuration of the Meridian LMS application.	• Provide MERIDIAN confirmation of functionality is configured within Stage/Production environments.
Assumptions	**Acceptance Criteria**
• CLIENT to configure desired base/custom views and database object relationships through configuration console that are not currently exposed via the identified base product views. • MERIDIAN will conduct and support five (5) days of Customer Acceptance Testing for all tasks defined in section B herein.	• Confirmation that the Meridian AdHoc functionality has been correctly configured and is functioning per the Requirements specified in task B.2 herein.

14. Optional Setup Tasks: Training

The purpose of this task is to provide additional training during the project implementation, based upon additional standard modules, or features implemented, per the scope defined herein. The description of these trainings and the number of respective days is provided below. Training can be purchased at a fixed fee of $ per day.

Training Types Definitions

- o Ad Hoc Report: (not in scope) - The purpose of this Ad Hoc Report training is to provide guidance on how to configure the Ad Hoc Report Builder and create custom reports.
- o Train-the-Trainer: (not in scope) - Training to train Client Trainers on the effective ways to train the system to End Users and various audiences.
- o Technical: (not in scope) - Training on how to manage integration with the Meridian system.
- o End User: (not in scope) - Training for end users on how to access the system, general navigation, and feature set review.
- o Additional Administrative: (not in scope) – The purpose of Administrative training is to provide the in-depth knowledge necessary to support administration system features and functions for the set up and management of the Meridian Learning Management System.

MERIDIAN Deliverables	CLIENT Deliverables
• Conduct required training sessions as depicted herein.	• Provide list of trainees, location(s), and training equipment in order to facilitate

MERIDIAN Deliverables	CLIENT Deliverables
• Printed Student Guides for up to twelve (12) people.	a hands-on training and demonstration of product features and functionality. • Pre-approval of travel reimbursement, if onsite instructor led training is required.
Assumptions	**Acceptance Criteria**
• No more than twelve (12) people. • Travel costs are not included in the cost. • A minimum of two (2) weeks' notice is required prior to the scheduling of training in order to appropriately manage resource schedules and minimize travel costs/impacts. • End User Training is not provided within the current scope of services. • Train-the-Trainer Training is not provided within the current scope of services. • Technical Training is not provided within the current scope of services.	• Delivery of the scoped number of days of training by type.

Training Cancellation Policies

Rescheduling or cancellations may result in a cancellation fee per the following schedule, plus any reasonable and necessary expenses incurred as a result of preparing to deliver the training described herein. Notification of a cancellation or reschedule must be made to MERIDIAN in writing.

- o More than twenty 20 business days prior to training – 0% of standard Training fee.
- o 11-20 business days prior to training start – 25% of standard Training fee.
- o 6-10 business days prior to training start – 50% of standard Training fee.
- o 0-5 business days prior to training start – 100% of standard Training fee.

C. Project Schedule

The scope of the implementation services as depicted herein is limited to a one (1) phase software deployment, estimated to take sixteen (16) weeks.

Schedule is dependent on CLIENT's ability to:

1. Complete all Discovery and Planning activities per the mutually agreed upon baselined Project Plan, including but not limited to:

a. Data Template Completion.

2. Provide Configuration and Integration Requirements in a timely manner.
3. Provide feedback on all loaded data in a timely manner.
4. Execute Customer Acceptance Testing activities per the agreed upon Project Plan.

A draft Project Plan will be provided within one (1) week after the Project Kick-Off date. The detailed Project Plan is subject to modification during the software implementation lifecycle with the mutual agreement of both the CLIENT and MERIDIAN.

D. Roles and Responsibilities

MERIDIAN and CLIENT agree to staff the Project at levels and conditions as set forth in the mutually agreed upon Project Plan. At a minimum, across all tasks as defined in section B.2 above, the Project will be staffed as follows:

MERIDIAN Resources

Role	Responsibilities	Participation	Skill Set
Project Manager	• Acts as Meridian's single point of contact throughout the project. • Develops and manages project plan. • Manages project issues and mitigates risk on behalf of Meridian. • Prepares for and conducts status meetings. • Provides status reports and financial tracking. • Conducts Requirement Confirmation Workshops. • Participates in and coordinates design, configuration, development, testing and deployment activities. • Note: In most cases, the Meridian Project Manager is not fully dedicated to one specific customer deployment since the	• Deployment Stages. • Discovery. • Execute. • Deploy. • Warranty. • Workstreams • Project Mgmt. • Software Setup. • Meridian University.	• Project Management experience managing teams, issues, project schedules and financials. • Meridian LMS configuration skills. • Process definition skills.

	responsibility does not require a full-time resource.		
Technical Solutions Architect	• Conduct Requirement Confirmation workshops to gather in-scope product extension requirements for complex projects only. • Drives the joint project team to a solution to meet all requirements in the most efficient and constructive manner. • Participates in execution of software development and testing activities.	• Deployment Stages. • Discovery. • Execute. • Warranty. • Workstreams • Software Setup.	• Meridian LMS product features & functionality expert. • Industry Business Process expert. • SQL database skills. • SQL query skills. • Process definition skills. • Data analysis skills. • Data conversion skills.
Implementation Consultant	• Facilitates end-user and system admin Requirements Gathering Sessions. • Confirms configuration requirements. • Identifies gaps and works with integrated team to develop resolutions. • Performs data conversion and migration activities. • Configures and tests software per defined requirements.	• Deployment Stages. • Discovery. • Execute. • Deploy. • Warranty. • Workstreams. • Software Setup.	• Meridian LMS product configuration skills. • In-depth Industry and process knowledge. • SQL query skills. • Process definition skills. • Data analysis skills.
Application Developer	• Establishes technical environments. • Extends software for requirements not supported by out-of-the-	• Deployment Stages. • Discovery. • Execute. • Deploy.	• Meridian LMS development expert. • SQL database skills. • SQL query skills.

	box features & configurations. • Configures/Develops integrations with the product per defined requirements.	• Warranty. • Workstreams. • Software Setup.	• .NET development skills. • Meridian LMS technical infrastructure skills.
Account Manager	• Analyzes and assesses client's maturity level and skill sets. • Assesses client's business processes and goals. • Creates recommendations to drive the maturity and the business forward. • Establishes and tracks strategic initiatives.	• Workstreams. • Post Deployment.	• In-depth Industry knowledge. • In-depth knowledge of industry best practices. • Strategic planning. • Project/Account Management. • Process definition and development skills. • Enablement and communications expert.
Meridian Trainer	• Delivers Implementation Readiness and LMS Administrator training. • Tailors training delivery to meet customer's business requirements and/or configuration decisions. • Finalizes training logistics.	• Deployment Stages. • Discovery. • Execute. • Workstreams • Meridian University.	• Meridian LMS product features & functionality expert. • In-depth knowledge of industry best practices.

E. Cost Estimate

Item Description	Cost
Standard Software Setup	$
Installation of Meridian LMS Environments	included
Discovery Session/Joint Requirements Development (JRD)	Included
Configuration & Branding Application	Included
System Integration	Included

Production Installation	Included
Training	Included
Go Live Support	Included
Optional Software Setup Tasks	$XXXXXXXXX
Historical Data Migration	$
Single Sign-On	$
eCommerce Integration	$
Meridian Social Setup	$
Meridian Mobile	$
AdHoc Setup	$
Additional Training	$/Day

ASSUMPTIONS:

1. All Services are an estimate based on the understanding of the scope of work. Implementation Services may vary based on increased domains, user audience, and scope, or time changes. Any additional Services that are identified through the workbook process (additional modifications, integrations, professional services support or consulting) can be added to this Agreement as needed or in a later CO SOW.
2. All pricing for additional scopes of work is valid for ninety (90) calendar days from the date of submission to the CLIENT.
3. Travel costs are not included in the Cost Estimate and will be invoiced per MERIDIAN'S current travel guidelines.

F. Out of Scope

The following is currently deemed outside of the scope for this implementation:

- Migrations, integrations, modifications to the system that are not explicitly included in the scope of this SOW.
- Custom reports, localization, documentation, or online help.
- Content cleansing, migration, or uploading unless specifically identified.
- Consulting or professional services not specified in the implementation tasks (i.e. courseware development, courseware troubleshooting, SCORM, HW/SW configurations or internal network setup or maintenance).
- Advanced Graphical design or other advanced (e.g. flash) GUI support.
- Editable training materials such as instructor and student guides.

G. Change Management

MERIDIAN recognizes that changes are a normal part of the project life cycle. Changes to the scope or timeline of the Services contemplated by this Agreement will require a formal Change Order Statement of Work ("Schedule 2") to be submitted by the MERIDIAN Project Manager

to the CLIENT. Changes in scope may include an increase in cost and/or timeline and will be specified in each change request. Prior to beginning the change request, CLIENT must execute the Schedule 2 Change Order. MERIDIAN requires formal change acceptance before beginning work on any changes. Changes within the defined scope of the contract need approval by the CLIENT Project Manager and the MERIDIAN Project Manager. Acceptance for scope changes, are given when both the CLIENT Project Manager and the MERIDIAN Project Manager formally approve the change by signing off on Schedule 2 so that miscommunications are avoided. Project change procedure is as follows:

i. Identify change (can originate from the CLIENT Project Manager or the MERIDIAN Project Manager);
ii. MERIDIAN completes Change Request Form;
iii. MERIDIAN Project Manager determines the impact of the proposed change (schedule, resources, time, and/or cost);
iv. MERIDIAN Project Manager submits Schedule 2 to the CLIENT Project Manager for review/approval.
v. MERIDIAN Project Manager receives approval from the CLIENT Project Manager within three (3) business days; and
vi. MERIDIAN Project Manager modifies or, if necessary, re-baselines the Project Schedule and Plan to include the approved change.
vii. Work begins as agreed upon to incorporate change; or,
viii. MERIDIAN Project Manager works with the CLIENT Project Manager to either adjust the requirements or revise the workload distribution, documenting all changes on a revised Change Request Form.

Change Management Criteria are as follows:

i. Any change that is outside the scope of effort defined in Schedule 1;
ii. Any additional deliverable or service not defined in Schedule 1, or changes to an accepted deliverable;
iii. Any subsequent modifications to an approved Change Request;
iv. Modifications to the technical or management approach defined in Schedule 1;
v. Any change in workload or environment or application inventory;
vi. Any additional activity or task not defined in Schedule 1 for a planned deliverable;
vii. A contradiction to items, assumptions or responsibilities stated in Schedule 1;
viii. A delay in turnaround of approvals, information, answers to questions; and
ix. Time lost due to reasons such as unavailability of equipment, software, or access to environment/infrastructure needed by the project team.

H. Acceptance Management

In an effort to avoid schedule delays stemming from delayed approvals of dependent tasks, MERIDIAN and CLIENT will mutually define a reasonable acceptance review period that does

not jeopardize the project duration as outlined within the project management support period. Delays in accepting project deliverables could result in a schedule slippage equaling as much as one day for every day acceptance review is delayed. Below are the methods used to verify and validate each of the defined deliverable(s).

i. **Deliverable Review and Approval.** MERIDIAN will provide deliverables to the CLIENT. Documentation deliverables will be provided to CLIENT in electronic form. A Deliverable Acceptance Form will be submitted to the CLIENT Project Manager for each deliverable. CLIENT will provide MERIDIAN with one set of consolidated comments. MERIDIAN will provide a CLIENT Quality Control (QC) sheet that may help the CLIENT collate all comments prior to delivering to MERIDIAN. The deliverable will be deemed acceptable when it satisfies the acceptance criteria specified for each deliverable or service or within ten (10) calendar days if no response is received. The Deliverable Acceptance will be signed and returned to MERIDIAN upon review of the deliverable within the mutually defined period as stated upon under acceptance management. In the event that the CLIENT rejects a deliverable, MERIDIAN will resubmit the deliverable to the CLIENT with the required changes within a mutually agreed upon timeline.

ii. **Acceptance Authority.** CLIENT will specify a single point of contact with deliverable acceptance/sign off authority. Sign off acceptance is required for deliverable by the approving authority, prior to moving any customizations to the production site.

iii. **Withholding Acceptance.** CLIENT shall not unreasonably withhold acceptance. If Acceptance is not granted or rejected within the mutually agreed upon timeframe, automatic Acceptance will be granted. In the event that failure to provide Acceptance extends the timeframe of the implementation activities within the respective Schedule 1, CLIENT may be liable for additional Project Management time in order to extend the schedule.

iv. **30 Day Post-Delivery Warranty.** After sign-off approval has been received, and MERIDIAN has delivered the files, CLIENT will have thirty (30) calendar days in which to report any production errors to the Project Manager. MERIDIAN will assess the error and correct as long as the error is within the scope of the original task completed. After thirty (30) calendar days from the date the files were delivered to the CLIENT, MERIDIAN will provide a cost estimate for any errors/revisions requested unless those costs are covered under separate sections of this Agreement. This warranty is only in terms of the work performed under the Exhibit A.

I. Invoicing Schedule

MERIDIAN will invoice Services based on the following deliverable milestones within the implementation timeline.

i. **Contract Execution [20%]** – Upon Contract Execution, twenty percent (20%) of the SOW fee will be invoiced.

ii. **Delivery to CLIENT Stage Environment [35%]** – At the point of all programmatic deliverables being released to the CLIENT Stage Environment for CLIENT review, the second thirty-five percent (35%) of the SOW fee will be invoiced.

iii. **Delivery to Production [35%]** – At the point of all programmatic deliverables being delivered for application to the Production Environment, thirty-five percent (35%) of the SOW fee will be invoiced.

iv. **Warranty Period Complete [10%]** – At the completion of the thirty (30) calendar day warranty period, the remaining ten percent (10%) of the SOW fee will be invoiced.

J. Additional Services – Labor Rates - RESERVED

K. Authorization

By signing below, CLIENT is authorizing MERIDIAN to move forward with the development and testing of the requested functionality, as detailed within this document. CLIENT agrees that the requirements, as documented herein, meet or exceed the expectation of the requested functionality.

Once signed, this page should be faxed or emailed to Meridian Knowledge Solutions, LLC:
To the attention of: Contracts
Fax #: 703.322.9568
Email contracts@meridianks.com

MERIDIAN: MERIDIAN KNOWLEDGE SOLUTIONS, LLC, a Virginia, limited liability company	CLIENT: <CLIENT_LEGAL_NAME> a <CLIENT_STATE_FULL>, <CLIENT_TYPE_OF_COMPANY>
By: Printed Name: Title: Date:_____	By: Printed Name: Title: Date:_____

SCHEDULE 2
SOFTWARE AS A SERVICE AND SUBSCRIPTION AGREEMENT

CHANGE ORDER TO SCHEDULE 1 - STATEMENT OF WORK #CO-001 (TEMPLATE)
IMPLEMENTATION OF THE MERIDIAN LMS
FOR <CLIENT_LEGAL_NAME>

This Schedule 2 is a Change Order to Schedule 1 – Statement of Work # SOW-001, dated <SOW_EFFECTIVE_DATE_MM/DD/YYYY> , and defines changes to the work to be provided under the terms and conditions of the Contract Agreement signed between MERIDIAN and CLIENT.

A. Effective Date of this Schedule 2

This Change Order is effective upon its execution by MERIDIAN and CLIENT. The estimated Change Order commencement date is **<CHANGE_ORDER_EFFECTIVE_DATE_MM/DD/YYYY>**.

B. Summary of Changes to the Scope of Implementation Professional Services

CLIENT has requested the following changes to the LMS implementation in support of **XXXXXXXXXXXXXXXXXXXXXXXX**

C. Authorization

By signing below, CLIENT is authorizing MERIDIAN to move forward with the development and testing of the requested functionality, as detailed within this document. CLIENT agrees that the requirements, as documented herein, meet or exceed the expectation of the requested functionality.

Once signed, this page should be faxed or emailed to Meridian Knowledge Solutions, LLC:

To the attention of:	Contracts
Fax #:	703-322-9568
Email	contracts@meridianks.com

SIGNATURE PAGE FOLLOWS

MERIDIAN:
MERIDIAN KNOWLEDGE SOLUTIONS, LLC,
a Virginia, limited liability company

By:
Printed Name:
Title:
Date:_____

CLIENT:
<CLIENT_LEGAL_NAME>
a <CLIENT_STATE_FULL>,
<CLIENT_TYPE_OF_COMPANY>

By:
Printed Name:
Title:
Date:_____

Cloud Solutions
Alternate Contract Source No. 43230000-NASPO-16-ACS

Contract Exhibit D

CONTRACTOR SELECTION JUSTIFICATION FORM

Customers must complete this Contractor Selection Justification Form and attach it to the Purchase Order.

Date: Click or tap here to enter text.

Contractor's Name: Click or tap here to enter text.

Service Model:

Saas ☐ PaaS ☐ IaaS[1] ☐

1 In accordance with Rule 60GG-3.004, F.A.C., "The acquisition of data center services, including IaaS, will be accomplished by customer entities submitting a Service Request to the State Data Center."

Level of Risk:

Low Risk Data ☐ Moderate Risk Data ☐ High Risk Data ☐

Description of Services:

Click or tap here to enter text.

Estimated Total Contract Value: Click or tap here to enter text.

Justification for Selection of Contractor:

Click or tap here to enter text.

Completed By: Click or tap here to enter text.

Title: Click or tap here to enter text.