BCBSM PARTICIPATION AGREEMENT

BETWEEN

[ENTITY] AND [SUPPLIER]

This Participation Agreement ("PA"), Contract ID# (XXXXX), contains the terms for the purchase and/or license of products and/or provision of services for the benefit of Blue Cross Blue Shield of Michigan ("Buyer"), whose address is 600 Lafayette East, Detroit, Michigan 48226. The Enterprise Master Services Agreement ("EMSA"), CID# (XXXXX), is incorporated into this PA.

1. Participation Agreement Exhibits

1.1. This PA includes the following exhibits, unless otherwise noted:

[Do not delete exhibit number. Replace exhibit name with "Intentionally Omitted" if any exhibit below will not be used]

a. Exhibit 1a – Master Statement of Work ("MSOW") Template
b. Exhibit 1b - Statement of Work ("SOW") Template
c. Exhibit 2 – Consulting Services Role Descriptions
d. Exhibit 3 – Rate Schedule (Intentionally Omitted or Time and Materials or Fixed Fee)
e. Exhibit 4 – Information Security Requirements
f. Exhibit 5 – Supplier Software License (To be added or intentionally omitted)
g. Exhibit 6 – Offshore Locations
h. Exhibit 7 – Service level Agreements ("SLA") Template to SOW/MSOW

2. Term of Participation Agreement

2.1. Term. This PA shall become effective on [EFFECTIVE DATE] ("Agreement Effective Date") and shall end on [EXPIRATION DATE] ("Term"), except as otherwise provided herein.

2.2. Performance. Unless Buyer by its designated Contract Administrator agrees in writing to an extension of time, Supplier shall complete any performance due under this PA before the Term ends. If, at any time, Supplier concludes it will be unable to complete performance before the end of the Term, Supplier shall immediately give the Buyer's Contract Administrator a complete explanation of the facts and reasons.

3. Termination

3.1 Termination for Convenience. Buyer, but not Supplier, may terminate this PA or any MSOW or SOW, in whole or in part, for its sole convenience upon fifteen (15) days' prior written notice. Supplier shall be paid for Services satisfactorily provided or performed prior to the effective date of termination. In no event shall Supplier be paid for costs incurred, anticipated profit, or support services performed after the effective date of termination.

3.2 Termination by Department of Health and Human Services. Buyer may terminate this PA immediately if the Department of Health and Human Services ("HHS") finds that Supplier has failed to satisfactorily perform Services in accordance with terms of this PA or any MSOW/SOW governed by this PA.

3.3 Termination for Change in Control. Supplier shall give Buyer prompt written notice of any announcement of a Change in Control of Supplier. Buyer may, at its option, terminate this PA upon receipt of such written notice. "Change in Control" shall be defined as (i) consolidation or merger of Supplier with or into any entity, (ii) sale, transfer or other disposition of all or substantially all of the assets of Supplier or (iii) acquisition by any entity, or group of entities acting in concert, of a controlling interest in Supplier. For purposes of this Section, "controlling interest" shall mean (A) beneficial ownership of twenty percent (20%) or more of the outstanding voting securities of the Supplier or (B) the right or power, whether by contract or otherwise, to direct Supplier's affairs or control Supplier's decisions, including without limitation the right or power to elect or appoint twenty

percent (20%) or more of the board of directors or other persons in whom is vested decision-making authority for Supplier.

3.4 Termination Effect on MSOW or SOW. The termination of this PA will not affect any MSOW/SOW that, by its own terms, extends beyond the effective date of termination of this PA, and the Parties will be bound by the terms of this PA until termination or expiration of the MSOW/SOW. The expiration or earlier termination of this PA will not relieve, release or discharge either Party hereto from any obligation, debt or liability that may have previously accrued and that remains to be performed as of the date of termination. The provisions of this section will survive the termination or expiration of this PA. Termination of this PA will be in addition to and not in lieu of any other remedies available to a Party in law or in equity.

3.5 Continued Performance. Each Party agrees to continue performing its obligations under this PA while any dispute is being resolved except to the extent the issue in dispute precludes performance (dispute over payment shall not be deemed to preclude performance).

4. Statements of Work and Services

4.1. Services. Assignments, tasks, products, functions or services provided by Supplier under this PA ("Services") shall be set forth in either a Master Statement of Work ("MSOW") or a Statement of Work or other mutually agreed contract document ("SOW"), in a format substantially similar to Exhibit 1. If any services, functions, or responsibilities are required for the proper performance and provision of the Services, regardless of whether they are specifically described herein, they shall be deemed to be implied by and included within the scope of the Services to be provided by Supplier to the same extent and in the same manner as if specifically described in this PA. Buyer must agree in writing to the Services prior to Supplier's commencement of any work under a MSOW/SOW. Supplier is a non-exclusive provider of the Services to Buyer, and Buyer may obtain similar services from other third parties. In providing the Services, Supplier shall provide all resources necessary for Supplier and its personnel to perform the Services (including personnel, software, tools, personal computers, hardware, circuits, equipment and facilities), except to the extent Supplier and Buyer agree otherwise in writing in a MSOW/SOW. The Services shall be performed in a manner, sequence and timing so as to coordinate with the work of Buyer's other contractors, suppliers and other consultants, if applicable, and Supplier agrees to cooperate in good faith with such third parties working on Buyer's behalf.

4.1.1. When Buyer engages Supplier on a **Time and Materials** basis under this PA, the following data elements will be provided: Role, Start and End Date, Hourly Rate (shall be set forth in Exhibit 3), Total Approved Amount. These data elements will be included in the SOW and/or Work Order (the SOW will exclude the Resource Name). At its discretion, Buyer may choose to issue a, SOW and Work Order or Work Order only, a Purchase Order will be issued for invoicing and administrative purposes. Changes in resources or adding funds to an executed SOW or Work Order will be completed by Buyer's Purchase Order only. Any material changes to the SOW shall be documented in an Amendment signed by both Parties.

4.1.2. When Buyer engages Supplier in reference to the **Fixed Rate or Not-to-Exceed Rate Schedule** in accordance with Exhibit 3, Buyer may choose to execute a MSOW/ SOW or issue a Purchase Order only. Any material changes to the MSOW/SOW shall be documented in an Amendment signed by both Parties.

4.2. Amendments. Supplier cannot make any changes to the Services without Buyer's prior written approval. Supplier must notify the Contract Administrator in writing within five (5) business days of Supplier's request for change to the MSOW/SOW. Supplier shall, at the time of delivering such notice, also provide the Contract Administrator with its proposed price adjustment, together with reasons and grounds in support. The Parties shall promptly confer to resolve whether a fee adjustment should be made, the changes are accepted by Supplier without additional cost or if Buyer's request should be withdrawn. Supplier considers a Buyer's amendment to any change of scope or deliverables.

4.3. Export. The Parties will comply with all export laws and regulations of the United States, including for "deemed exports", and all export controls applicable thereunder. To the extent within Supplier's control and as part of its provision of Services, Supplier shall be responsible for, and shall coordinate and oversee, compliance with such export laws in respect of such items exported or imported hereunder.

4.4. Entirety. This PA incorporates each MSOW/SOW in its entirety. The Parties agree that any MSOW/SOW provision that is inconsistent with this PA shall be of no force or effect and shall be disregarded and the PA provision take precedence, unless the MSOW/SOW expressly states otherwise; in order for a MSOW/SOW to modify or amend the PA or EMSA with respect to a particular MSOW/SOW, the modifying or amending term must be included within the "Override" section of the MSOW/SOW (and shall list the specific term from the PA or EMSA that it is intended to override). Any such modifying or amending terms shall applicable only to the MSOW/SOW in which such deviations are contained.

5. Government Programs

5.1. Supplier agrees to comply with the Government Programs provisions as revised from time to time. The current version thereof can be found by visiting the following the following site:, (Government compliance, Government Language Long Form (PDF) (FDR Suppliers)) https://www.bcbsm.com/content/dam/microsites/procurement/government-programs-requirements-long.pdf or (Government Language Short Form (PDF) (Non-FDR Suppliers)) https://www.bcbsm.com/content/dam/microsites/procurement/government-programs-requirements-short.pdf or (Government Language Long Form (PDF) (FDR Suppliers-PDP)) https://www.bcbsm.com/content/dam/microsites/procurement/government-programs-requirements-long-form-part-d.pdf where appropriate and is incorporated herein by reference. Buyer shall provide Supplier written notice of any revision thereto, and the revised version shall replace and supersede any and all prior versions.

6. Federal Employee Program and E-Verify

6.1. Supplier agrees to comply with the Federal Employee Program (FEP) Addendum ("FEP Addendum") provisions as revised from time to time. The current version thereof can be found by visiting the following site: https://www.bcbsm.com/content/dam/microsites/procurement/required-fep-contract-flow-down-provisions.pdf (under "Government Compliance, Required FEP Contract Flow-Down Provisions (PDF)"), and is incorporated herein by reference.

6.2. The FEP Addendum is a subcontract of a federal procurement contract with the United States Office of Personnel Management ("OPM"). As such, the FEP Addendum is subject to certain federal procurement clauses, the obligations of which must "flow down" to the Supplier.

6.3. Buyer may amend the FEP Addendum to include new or revised DOL, FAR and FEHBAR Flow-Down Clauses required under the OPM contract by providing thirty (30) days prior written notice of such amendment. Supplier's signature is not required to make any such amendment effective.

7. Supplier Personnel and Subcontracting

7.1. Supplier shall utilize, to perform the Services, employees and subcontractors (subject to Section 7.2 below) (collectively, "Supplier Personnel") who are properly educated, trained, experienced, and fully qualified for the Services they are to perform. Supplier Personnel shall be proficient in English. Supplier is responsible for having in place with all Supplier Personnel (either directly or indirectly through their respective employers) such agreements respecting Intellectual Property Rights as are necessary to comply with Section 8 (Intellectual Property) below.

7.2. Supplier shall not subcontract its obligations under this PA to any third-party company or individual unless Supplier provides Buyer with written notice and Buyer subsequently provides written approval of such

subcontractors. Supplier agrees that any subcontractor shall comply with all terms and conditions of this PA in the same manner as Supplier.

8. Intellectual Property

8.1. Reporting of Work Product. For purposes of this PA, "Work Product" means all original materials, tangible or intangible work product, and Deliverables developed, invented, discovered, created, authored, or otherwise originated (whether alone or jointly with others) under this PA. Supplier shall promptly disclose all Work Product to Buyer upon its development, invention, discovery, creation, authoring or origination.

8.2. Ownership of Work Product. Supplier agrees that all Work Product and all intellectual property rights therein shall be the sole and exclusive property of Buyer. Supplier agrees to assign and does hereby expressly assign and transfer to Buyer all right, title and interest worldwide in and to the Work Product and all intellectual property rights contained therein.

8.3. Works for Hire. All works of authorship forming Work Product shall be, to the extent possible, considered a "work made for hire" for Buyer under the United States Copyright Laws and are the sole and exclusive property of Buyer, and shall immediately vest in Buyer.

8.4. Assignment. To the extent that any such Work Product does not qualify as "work for hire" under applicable law, Supplier hereby irrevocably and exclusively assigns to Buyer all right, title and interest in and to all such Work Product, agrees to sign all necessary or appropriate documents to register the any intellectual property in the name of Buyer, and shall cause its personnel to assign, at the time of creation for the Work Product, without the right of any further consideration, all right, title and interest in or that they may have in such Work Product.

8.5. Pre-Existing Materials. To the extent that the Work Product includes materials existing as of the effective date of this PA, or materials of Supplier's licensors ("Pre-Existing Materials"), Supplier hereby grants to Buyer a perpetual, royalty-free, paid-up, irrevocable, transferable, sublicensable, worldwide, non-exclusive right and license to use, execute, reproduce publicly perform, display, modify, improve, create derivative works of, distribute, transmit, import, make, have made, sell and offer to sell and otherwise exploit any Pre-Existing Materials, including all such modifications, improvements and derivative works thereof, solely to the extent such Pre-Existing Materials are incorporated in, combined with or otherwise necessary or useful to use or exploit the Work Product for any purposes or reasonably required in connection with Buyer's receipt of the Work Product. Notwithstanding the foregoing, Supplier shall not incorporate any Pre-Existing Materials in any Work Product without prior written permission of Buyer.

8.6. Further Assistance. Supplier shall, upon request of Buyer, promptly execute a specific assignment of title to Buyer and do anything else reasonably necessary to enable Buyer to secure for itself any patent, trade secret or other proprietary rights in the United States or other countries relating to the Work Product. Such documents shall be prepared by Buyer, at Buyer's expense, and Supplier shall be required to sign them only upon the request of Buyer. All materials produced under this PA shall be and shall remain the property of Buyer, whether, or not registered.

9. Offshore

9.1. Supplier and any approved subcontractor shall not provide offshore services without the prior written consent of Buyer. This shall include, but is not limited to, any access or sending of confidential data, including Protected Health Information ("PHI") or Personally Identifiable Information (PII), as defined by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), to a location outside of the United States.

9.2. If Buyer agrees in writing and in advance that Services may be performed offshore, then Buyer may issue an MSOW, SOW or Purchase Order. In any event, Buyer will issue a Purchase Order for invoicing and administrative purposes. Supplier will update Exhibit 6 as offshore locations are modified and approved by

Buyer. Supplier shall complete and sign Buyer's Annual CMS or Non-CMS Form for all locations which identify Supplier offshore controls for PHI/PII or other confidential information when they are accessed, stored, hosted, viewed, or transferred.

9.3 The Offshore Rate Schedule reflects the following details in accordance to Exhibit 3, unless intentionally omitted.

10. Payment Terms

10.1. Payment terms are 2% 15/Net 60. Payment for a properly submitted invoice is due within 60 days after the invoice is received and approved by the buyer within the Oracle Supplier Portal. In the event Buyer makes payment on or before the 15th day after receiving the invoice, Buyer shall take a 2% discount from the invoice total as consideration for the prompt payment. Payment shall be considered made by Buyer on the date printed on the check or on the date Buyer transfers the invoice payment via electronic transfer method (e.g., EFT). In no event shall Buyer be liable to Supplier for any interest or late payment fees.

11. Annual Volume Rebate

11.1. During the term of this PA, the following annual volume rebate shall apply:

11.2. If the YTD Contract Volume, defined below in subsection 11.4, is $0 - $499,999, then the rebate shall be 4%. If the YTD Contract Volume is $500,000 or more, then the rebate shall be 6%.

11.3. The applicable volume rebate shall be applied by Supplier on an annual basis to all Services performed by Supplier when a specified volume is reached. Discounts are based on when the work was performed, not when invoices are received (for example, invoices received after January 1st for work performed prior to January 1st, fall into the discount structure of the year the work was performed).

11.4. The volume rebate shall be based on Buyer's total payments made and outstanding payables due for that calendar year ("YTD Contract Volume"). All amounts due to Buyer under this Section shall be paid in full by a check within one hundred twenty (120) days of the end of the just completed calendar year. Checks should be mailed to Blue Cross Blue Shield of Michigan, Attn: Accounts Payable, Mail Code 0811; 600 Lafayette East, Detroit, Michigan 48226. Supplier shall also email a copy of the annual volume discount check and/or invoice credit statement to the Contract Administrator and the Procurement Representative.

11.5. In the event Buyer is owed any amounts under this Section after the termination of this PA, Supplier shall pay Buyer the full amount owing by check no later than sixty (60) days after the date this PA is terminated.

11.6. Buyer is not required to purchase any specific volume of Services from Supplier during the term of this PA, and Buyer makes no commitment for any minimum volume, scope or value of the Services.

11.7. Supplier's obligations under this Section shall survive the term of this PA.

12. Diverse Supplier Requirement

12.1. Supplier agrees to comply with registering through the Tier II Diverse Supplier Portal and to report the use of diverse companies for its secondary spend. In addition, Supplier agrees to comply with a fifteen (15) percent diversity spend requirement throughout the term of this PA. All spend must be uploaded to the Tier II Diverse Supplier Portal on a quarterly basis according to program reporting guidelines. Registration on the portal must be completed within ten (10) business days of signing this PA and can be located through the following hyperlink: https://www.unifiedtier2.com/request-reporting-access.html

13. 508 Electronic Accessibility Compliance

13.1. Supplier agrees that if any of the Services being provided are a part of Buyer's health programs or activities provided through electronic means and/or information technology (e.g., website or mobile application), all content will be accessible to individuals with disabilities as required under Section 1557 of the Affordable Care Act and Section 508 of the Rehabilitation Act. Content must also and meet the most current the Web Content Accessibility Guidelines (WCAG) 2 requirements.

14. Non-Solicitation of Employees

14.1. With the exception of generalized recruiting practices, including but not limited to responses to advertisements, internet postings and job fairs, should either Party like to solicit an employee of the other Party to apply for regular employment, the Party shall contact the other Party's designated representative to determine if the employee is interested in pursuing an offer. If the employee is interested, the soliciting Party's representative shall work with the other Party to set up any needed meetings.

15. Notices

15.1. The Parties shall deliver any notice by U.S. first class overnight mail, or express overnight courier addressed to:

To Buyer: Attn: Contract Administrator, Corporate Procurement Department, Blue Cross and Blue Shield of Michigan, 600 Lafayette East, Mail Code: 0625, Detroit, MI 48226.

With copies to: Attn: Contract Manager, Contract Management Department, Office of the General Counsel, Blue Cross and Blue Shield of Michigan, 600 Lafayette East, Mail Code: 1915, Detroit, Michigan 48226.

If to Supplier: Notices shall be sent to the address listed in the Recital section of this PA unless otherwise specified herein.

SIGNATURES

BLUE CROSS BLUE SHIELD OF MICHIGAN:

By: _____

Name: _____

Title: _____ _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

SUPPLIER:

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 1a
(Template)
Master Statement of Work

(Project Name)

BETWEEN

ENTITY

AND

(SUPPLIER)

This Master Statement of Work, Contract ID# (XXXXX), and any attachments hereto ("MSOW"), is governed by the Enterprise Master Service Agreement ("EMSA"), CID# (XXXXX), and the Participation Agreement ("PA"), CID# (XXXXX) or Master Agreement (name of Master), CID# (XXXXX), between (insert Entity) ("Buyer") and (insert Supplier) ("Supplier"), effective (insert effective date of Master or PA) ("Agreement"). In the event that any term or condition in the MSOW conflicts with any term or condition in the Agreement, the Agreement shall control, unless otherwise stated herein.

Now, therefore, in consideration of their mutual promises, Supplier agrees to perform this MSOW as follows:

I. Scope of Work and Project Services

A. Project Overview. This MSOW describes the services and key deliverables on a general level to be performed and provided by Supplier for Buyer.

B. MSOW Term. This MSOW shall begin _____ __, 20__, and shall end _____ __, 20__.

C. Scope of Work.

1. **Description of Services.** "Services" are defined and shall be performed by the Supplier as follows:

2. **Description of Deliverables.** "Deliverables" are defined and shall be performed by the Supplier as follows:

3. **Roles and Rates.** "Roles and Rates" are set in accordance with the Participation Agreement and are listed as follows:

Role	Rate	Role	Rate
	$		$
	$		$
	$		$

4**. Service Level Agreements "SLA".** Refer to Exhibit 7. in the Participation Agreement to add in SLA's this MSOW.

D. Work Location. Work against this MSOW shall be performed at the following location: _____. Contract Administrator to determine if Supplier or Resource is located in the United States or Offshore. Any Non-domestic request will require the physical address.

E. Subcontractors. By executing the MSOW**,** Supplier attests its Subcontractors, and its Subsidiaries shall abide by all terms and conditions of this MSOW and Agreement. Buyer consents to the following Subcontractors:

Subcontractor and/or Subsidiaries legal Name	Services	Are Services being performed Offshore? (Y/N)

F. Warranty Terms. Supplier warrants that work against this MSOW is warranted for 12 months after receipt of final payment by Buyer ("Labor Warranty"). In addition, Supplier warrants that all Services performed against this MSOW are warranted for a period of 12 months after receipt of final payment by Buyer ("Materials Warranty").

II. Payment and Payment Milestone Conditions

A. Pricing Schedule. The pricing for this Fixed Fee MSOW shall be as follows:

1. The Services under the Master Statement of Work (MSOW) shall be performed in accordance with the following services listed below. Pricing is set in accordance with the Participation Agreement.

Description of Services	Price
	$
	$

2. Any material changes not reflected in the PA and/or MSOW require written approval by the Contract Administrator including an Amendment to the PA and/or MSOW. Buyer may increase funding by issuing a Purchase Order to Supplier.

B. Key Personnel

Buyer Key Personnel		Supplier Key Personnel	
Resource Name	**Resource Title**	**Resource Name**	**Resource Title**

C. **Total Amount of MSOW.** The total billable amount of this MSOW shall not exceed $_____U.S. Dollars unless agreed in writing by both parties through the issuance of a PO by Buyer

D. Final Inspection and Acceptance. Buyer shall inspect all Services completed by Supplier under this MSOW. The Contract Administrator must provide written acceptance that the Services have been completed by Supplier as required under this MSOW. If the completed Services have not been accepted by the Contract Administrator, Supplier agrees to provide, at no additional cost to Buyer, all necessary resources, including but not limited to materials, permits, and services required. This shall continue until the Contract Administrator provides written acceptance of such Services.

III. Buyer Administrative Details

A. Contract Administrator. The Buyer Contract Administrator for the MSOW is _____.

B. Purchase Order Number. Buyer shall assign a Purchase Order number after the execution of this MSOW for administrative and invoicing purposes. All Supplier invoices shall include the assigned Purchase Order number.

C. Invoices. All Invoices shall be submitted through the Oracle Supplier Portal against the assigned Purchase Order number to this MSOW and shall be emailed to the Contract Administrator _____.

IV. Supplier Attestation

By executing this MSOW, Supplier attests that as of the effective date of this MSOW, Supplier is in compliance with the Government Programs provisions set forth in the Agreement, including all requirements relating to checking the OIG List and GSA List (as those terms are defined in the Agreement).

SIGNATURES

This Master Statement of Work is agreed to by both parties as witnessed by their respective signatures below. By signing this Master Statement of Work, the signatory for each party hereby certifies and represents that he or she has the actual authority to bind their respective party to this MSOW.

BLUE CROSS BLUE SHIELD OF MICHIGAN	SUPPLIER
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

By: _____

Name: _____

Title: _____

Date: _____

Exhibit 1b
(Template)
Statement of Work XX-XXXXX
(Insert project name)

BETWEEN

BLUE CROSS BLUE SHIELD OF MICHIGAN
An Independent Licensee of the
Blue Cross and Blue Shield Association

AND

SUPPLIER

This Statement of Work #XX-XXXXX, Contract ID# (XXXXX), and any attachment(s) hereto ("SOW"), is governed by the Enterprise Master Service Agreement ("EMSA"), CID # (XXXXX), and the Participation Agreement ("PA"), CID # (XXXXX) or Master Agreement (name of Master), CID# (XXXXX), between Blue Cross Blue Shield of Michigan ("Buyer") and (insert Supplier Name) ("Supplier"), effective (effective date of Master Agreement or PA) ("Agreement"). In the event that any term or condition in this SOW conflicts with any term or condition in the Agreement, the Agreement shall control.

Now, therefore, in consideration of their mutual promises, Supplier agrees to perform this SOW as follows:

I. Scope of Work and Project Deliverables

A. Project Overview. This SOW describes the services and key deliverables on a general level to be performed and provided by Supplier for Buyer (Contract Administrator to include a 2-3 sentence summary of the SOW)

B. SOW Term. This SOW shall begin _____ __, 20__, and shall end _____ __, 20__.

C. Scope of Work.

1. Description of Services. "Services" are defined and shall be performed by the Supplier as follows:

Supplier Services	Deliverables

2. Service Level Agreements "SLA". Define any SLA's measurements and Penalties in an Exhibit A. to this SOW.

D. Work Location. Work against this SOW shall be performed at the following locations: _____. Contract Administrator to determine if Supplier or Resource is located in the United States or offshore. Any non-domestic requests will require the physical address.

E. Subcontractors. By executing the SOW, Supplier attests its Subcontractors shall abide by all terms and conditions of this Agreement. Buyer consents to the following Subcontractors**.**

Name of Subcontractor	Services	Are Services being performed Offshore? (Y/N)

F. Warranty Terms. Supplier warrants that work against this SOW is warranted for 12 months after receipt of final payment by Buyer ("Labor Warranty"). In addition, Supplier warrants that all Services performed against this SOW are warranted for a period of 12 months after receipt of final payment by Buyer ("Materials Warranty").

II. Payment and Payment Milestone Conditions

A. Pricing Schedule. The pricing for this [Fixed Fee SOW] or [Time and Materials SOW] shall be as follows:

Milestone	Deliverables	Payment	Deliverable Due Date
Total			

B. Total Amount of SOW. The total billable amount of this SOW shall not exceed $___ U.S. Dollars. Buyer may increase funding by issuing a Purchase Order to Supplier.

C. Final Inspection and Acceptance. Buyer shall inspect all services completed by Supplier under this SOW. The Contract Administrator must provide written acceptance that the services have been completed by Supplier as required under this SOW. If the completed services have not been accepted by the Contract Administrator, Supplier agrees to provide all necessary materials, permits, and services required at no additional cost to Buyer until the Contract Administrator provides written acceptance.

III. Buyer Administrative Details

D. Contract Administrator. The Buyer Contract Administrator for the SOW is _____.

E. Purchase Order Number. Buyer shall assign a Purchase Order number after the execution of this SOW for administrative and invoicing purposes. All Supplier invoices shall include the assigned Purchase Order number.

F. Invoices. All Invoices shall be submitted through the Oracle Supplier Portal against the assigned Purchase Order number to this SOW and shall be emailed to the Contract Administrator _____.

IV. Supplier Attestation

A. By executing this SOW, Supplier attests that as of the effective date of this SOW Supplier is in compliance with the Government Programs provisions set forth in the Agreement, including all requirements relating to checking the OIG List and GSA List (as those terms are defined in the Agreement).

In addition to the preceding language, the following section should be used for a Time and Materials SOW (DELETE the following Sections 1 through 3, if this SOW is not being used for a Time and Materials SOW).

1. Buyer may generate an electronic invoice in its STP system on behalf of Supplier for the service(s) performed by first Wednesday of the month following the preceding financial month based on the Supplier's invoice cycling date. Buyer shall approve and pay the invoice based on the established payment terms and the current calendar year invoicing schedule with Supplier. If timesheet submission is required in the applicable time reporting tools, invoices will be created based off the approved time and paid in accordance with your payment terms.

2. **Professional Fees.** The Services under this SOW shall be performed in accordance with the following Roles and Hourly Rate(s). Changes to any role or rate below requires written approval by the Buyer's Contract Administrator and an Amendment to this SOW.

Role	Hourly Rate
EXAMPLE: Consultant, Advanced	$

3. **Insert Roster Language.** The services under this SOW shall be performed on a time and materials basis in accordance with the billable rates and hours detailed in the Resource Roster for this SOW. Independent Contractor shall complete the initial Resource Roster prior to execution of this SOW. Changes to the Resource Roster requires written approval by the Buyer Contract Administrator and Independent Contractor. Buyer Contract Administrator, or Delivery Lead shall submit a new Resource Roster including the changes to Independent Contractor personnel to Contingent Labor Contingentlabor@bcbsm.com no later than seven (7) days prior to the effective date of the change. Buyer is not liable to pay for any labor performed by resources not on a fully approved Resource Roster on or before the resources start date. Resources that are not included on this Resource Roster shall not be entered into Buyer's time reporting tool (STP or other).

The above Agreement is agreed to by both parties as witnessed by their respective signatures below. By signing this Agreement, the signatory for each party hereby certifies and warrants that he or she has the actual authority to bind their respective party to this Agreement.

SIGNATURES

BLUE CROSS BLUE SHIELD
OF MICHIGAN

By: _____TEMPLATE_____

Name: _____

Title: _____

Date: _____

By: _____TEMPLATE_____

Name: _____

Title: _____

Date: _____

SUPPLIER NAME

By: _____TEMPLATE_____

Name: _____

Title: _____

Date: _____

EXHIBIT 2
Consulting Services Role Descriptions

Consultant, Associate - Generally operating in a strategic capacity, works with line management to evaluate existing systems and/or end-user needs to design, recommend, and assist in the implementation of complex system changes. Familiar with a broad range of IT concepts, practices, and procedures. Relies on experience and judgment to plan and accomplish goals. Performs a variety of complicated tasks. Creates value for an organization through the application of knowledge, techniques, and assets to improve business performance. May involve providing objective appraisals where it is often easier for an expert outsider to see the broader picture. Typically required to summarize and present findings to audiences of various organizational levels. Engagements are typically no longer than 12 months. Bachelor's degree is not required but expected. At least 5-7 years of experience in business and IT roles preferred.

Consultant, Advanced - Generally operating in a strategic capacity, works with senior management to evaluate existing complex systems and/or end-user needs to design and recommend an optimal strategic direction for business systems. Familiar with a broad range of IT concepts, practices, and procedures. Relies on experience and judgment to plan and accomplish goals. Performs a variety of complicated tasks. May lead and direct the work of others for limited periods. Frequently reports directly to an executive or a senior project manager. Creates value for an organization through the application of knowledge, techniques, and assets to improve business performance. May involve providing objective appraisals where it is often easier for an expert outsider to see the broader picture. Typically required to summarize and present findings to executive levels. A wide degree of creativity, independence, and latitude is expected. Engagements are typically no longer than 6-8 months. Bachelor's degree is not required but expected. Master's degree preferred. At least 8-10 years of experience in business and IT consulting roles preferred.

Consultant, Senior - Generally operating in a non-routine and strategic capacity, works with senior management to evaluate existing systems and/or end-user needs to design and recommend an optimal strategic direction for business systems. Conclusions are objective, logical and based on facts that have been carefully collated and verified. Recommendations, however, are subjective and based on the consultant's background and experience. Knowledgeable of a broad range of business and IT concepts, practices, and procedures. May lead and direct the work of others with capabilities to manage very large projects. Frequently reports directly to an executive. Creates value for an organization through the application of knowledge, techniques, and assets to improve business performance. Provides objective appraisals as an expert outsider who provides a broader picture perspective. Typically required to summarize and present findings to executive levels. A wide degree of creativity, independence, and latitude is expected. Some knowledge of Buyer technologies and/or business verticals. Engagements are typically no longer than 3-6 months. Bachelor's degree is required. Master's degree is not required but expected. A minimum of 10-15 years of experience in business/IT consulting roles within large corporations preferred.

Consultant, Executive -- Senior level consultant who holds a multi-perspective viewpoint (industry, IT, operations) related to relevant business and technology issues. Operating in a strictly strategic capacity with a broad view of the organization, gives independent and objective advice on how best to use information technology to approach business challenges. Work will often be based on the need to improve efficiency and the way a company functions, frequently with IT used to achieve this. Conclusions are objective, logical and based on facts that have been carefully collated and verified. Recommendations, however, are subjective and based on the consultant's extensive background and experience. An expert in a broad range of business and IT concepts, practices, and procedures. Frequently leads and directs the work of others with capabilities to manage enterprise-level projects. Typically reports directly to the CEO, COO, or CIO. Creates value for an organization through the application of knowledge, techniques, and assets to improve business performance. Provides objective appraisals as an expert outsider who provides a broader picture perspective. Knowledgeable of emerging technologies, trends, and best practices. Typically required to summarize and present findings to large groups and/or executive levels. Strong knowledge of Buyer technologies and/or business verticals. Engagements are typically less than 120 days. Bachelor's degree is required. Master's degree is not required but expected. A minimum of 15 years of experience in business/IT consulting roles within large corporations preferred.

EXHIBIT 3
Rate Schedule

TIME AND MATERIALS or FIXED FEE (delete the one that does not apply)

A. TIME AND MATERIALS

The Services under the Statement of Work (SOW) shall be performed in accordance with the following Roles and Hourly Rate(s), and Resource's Location (onshore/Offshore). Changes to any role or rate below requires written approval by the Buyer Contract Administrator and an Amendment to the SOW.

Buyer and Supplier agree to the following Rate Schedule, which sets forth the rates per hour for each Supplier resource level delivering Services. Supplier's rates, as of the Effective Date, and/or as amended, are referred to as the "Rates." This Rate Schedule is made effective upon the execution of the Agreement and shall remain in effect until the termination of the Agreement; or until an adjusted Rate Schedule is agreed to in writing by both parties. Any adjustment to the Rate Schedule must be mutually agreed to, in writing, by Buyer's Corporate Procurement Department and Supplier, and shall not become effective until signed by Buyer 's Corporate Contract Administrator in the form of an Amendment to this Agreement. All Rate Schedule Amendments shall be numbered sequentially and contain the heading "Rate Schedule Amendment # ___" and indicate the effective dates. Buyer shall pay Supplier on a monthly basis for all Services completed during the prior month and approved by Buyer's Contract Administrator. Changes during the term of the controlling Agreement shall be set forth in the Rate Schedule through an Amendment and reflected below.

Role/Title	Hourly Rate	Resource Location Offshore (Y/N)
	$	

B. FIXED FEE

The Services under the Master Statement of Work (MSOW) or Statement of Work (SOW) shall be performed in accordance with the following Description of Service(s) and Rate(s), and Work Location (Onshore/Offshore). Changes to any Description of Service or Rate below requires written approval by the Buyer Contract Administrator and an Amendment to the MSOW/SOW. Changes during the term of the controlling Agreement shall be set forth in the Rate Schedule through an Amendment and reflected below.

Description of Service(s)	Rate	Work Location Offshore (Y/N)
	$	

EXHIBIT 4
Information Security Requirements

1. Purpose

1.1. This Information Security Requirements document describes the minimum information security requirements that Supplier shall comply with in performing services for, or otherwise accessing data belonging to, the contracting entity or entities ("Buyer") identified on the applicable EMSA, Participation Agreement, Business Associate Agreement, Statement(s) of Work or any other related document (collectively, "Agreements"). All capitalized terms not defined herein shall have the meaning set forth in the Agreements.

2. Information Security Management Program

2.1. Supplier shall have an Information Security Management Program ("ISMP") that addresses the overall security program of Supplier. The ISMP shall be formally documented, and such records shall be protected, controlled, and retained according to federal, state, and internal requirements.

2.2. Supplier management support for the ISMP shall be demonstrated through signed acceptance or approval by Supplier's management.

2.3. Buyer shall have the right to assess with reasonable notice the effectiveness of the ISMP by reviewing Supplier's information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions, and management support at least annually.

3. Access Control

3.1. Access Control Policy. Supplier shall establish, document, and communicate to Buyer a formal access control policy based on business and security requirements for access. Access control rules shall account for and reflect Supplier's policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users shall be clearly stated. Access controls must be both logical and physical. Users and service providers shall be given a clear statement of the business requirements to be met by access controls. The policy shall be reviewed at least annually and updated as needed to ensure accuracy and effectiveness.

3.2. Review of User Access Rights. All access rights shall be regularly reviewed by Supplier's management through a formal documented access review process.

3.2.1. User Registration. Supplier shall implement and document a user registration and de-registration procedure for granting and revoking access. User account types shall be identified, and conditions for group and role membership shall be established.

3.2.2. User Identification and Authentication. Supplier shall require users to have unique identifiers ("user IDs") for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of the user. Supplier shall provide a list of all user accounts that will have access to PHI on an as-needed basis. Authentication and authorization mechanisms shall be applied for users and equipment.

3.2.3 User Attestation: Supplier shall perform, at least bi-annually, perform an all-user attestation process. The User Attestation process is an ongoing review and confirmation of appropriate user access that will correlate users with their access to systems and applications.

3.2.4. Privilege Management. Supplier shall restrict and control the allocation and use of privileges to information systems and services through a formal authorization process. Privileges shall be allocated to users with minimum necessary access to perform their job role and responsibilities.

3.3. Secure Log-on Procedures. Supplier shall control user access to operating systems with secure log-on procedures that will display general notice warnings that computers may: (i) only be accessed by authorized accounts; (ii) limit the number of unsuccessful log-on attempts; (iii) enforce recording of

unsuccessful attempts; (iv) force time delay before further log-on attempts are allowed; (v) reject any further attempts without specific authorization from an administrator; and (vi) not display the password being entered by hiding the password characters and symbols.

3.3.1. Password Management. Supplier shall ensure that passwords are controlled through a formal management process. Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of strong passwords.

3.3.2. User Authentication for External Connections. Supplier shall develop and implement appropriate authentication methods to control access of remote users to systems containing sensitive information by requiring the use of password or passphrase and at least one (1) of the following: a cryptographic-based technique, biometric techniques, hardware tokens, software tokens, a challenge/response protocol or certificate agents.

3.4. Network Services and Connection Control. Supplier shall specify the networks and network services to which users are authorized to access. Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. The capability to connect to shared networks shall be restricted in line with the access control policy and requirements of the business applications.

3.4.1. Equipment Identification in Networks. Supplier shall use automatic equipment identification to authenticate connections from specific locations and equipment to determine whether they are permitted to connect to the Supplier's network.

3.4.2. Remote Diagnostic & Configuration Port-Protection. Supplier shall implement controls restricting physical and logical access to diagnostic and configuration ports from unauthorized use. Access controls to diagnostic and configuration ports shall include but are not limited to key locks, access-controlled badges, and other access restriction mechanisms Ports, services and similar applications installed on a computer or network systems, which are not specifically required for business functionality, shall be disabled or removed.

3.4.3. Segregation in Networks. Groups of information services, users and information systems shall be segregated on networks.

3.4.4. Network Protection. Supplier shall implement and maintain firewalls and intrusion detection or protection systems, which will forward event data and security alerts to a centralized system information and event monitoring ("SIEM") system for analysis, reporting and incident response. Supplier shall perform firewall configuration and access control list reviews on at least ~~a~~ monthly basis, to ensure appropriate controls and configurations are applied to limit traffic to only what is required for business operations within networks such as internal, external, and any demilitarized zone (DMZ).

4. Human Resources Security

4.1. Roles & Responsibilities. Supplier shall define and document the security roles and responsibilities of employees, contractors, and third-party users in accordance with Supplier's information security policy. Supplier shall ensure that workforce members agree to terms and conditions related to information security where it is appropriate to the nature and extent of access, they will have to Supplier's assets associated with information systems and services.

4.2. Terms and Conditions of Employment. Supplier shall ensure that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to Buyer's assets associated with information systems and services.

4.2.1. Screening. Supplier shall conduct background verification checks on all candidates for employment, current employees, contractors and third-party users in accordance with relevant

laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

4.2.2. Disciplinary Process. A formal disciplinary process shall be established and implemented for employees who have violated security policies and procedures.

4.2.3. Removal of Access Rights. The access rights of all employees, contractors, and third-party users to information and information assets shall be removed upon termination of their employment or modified upon a change of employment. Changes of employment or other workforce arrangements shall result in a removal of all access rights that are not required for the new employment or workforce arrangement.

4.3. Information Security Awareness, Education and Training. Supplier shall ensure that all employees, contractors, and third-party users receive appropriate awareness training and regular updates in Supplier's policies and procedures as relevant to their job function.

5. Risk Management

5.1. Risk Management Program. Supplier shall create and implement a comprehensive program that manages the risks to information system operations, assets, and Buyer information. The risk management program shall develop means through which the Supplier shall manage and mitigate risks to Buyer, including but not limited to physical and environmental hazards.

5.2. Risk Assessments. Supplier shall perform risk assessments to identify information security risks. Risk assessments are to be performed at least annually or when major changes occur in the environment, and the results shall be reviewed at least annually. Suppliers shall either remediate and/or provide a documented remediation plan for any critical risks that are identified as a result of the vendor security risk assessment.

6. Information Security Policy

6.1. Information Security Policy. Supplier shall develop, publish, and implement information security policy documentation. The information security policy shall include the purpose and scope of the policy, describe management's and workforce member's roles and responsibilities, and establish Supplier's approach to managing information security. The policy documents shall be reviewed at least annually and updated as needed. to ensure the policies' adequacy and effectiveness.

7. Organization of Information Security

7.1. Confidentiality Agreements. Supplier shall ensure that all personnel who access Buyer's data will sign confidentiality or non-disclosure documents with Supplier that comply with the applicable legal and security requirements outlined in the agreements.

7.2. Independent Review of Information Security. Supplier shall review at least annually, which may also include when significant changes to the security implementation occur, Supplier's approach to managing information security and its control objectives, controls, policies, processes, and procedures. The review shall include an assessment of Supplier's adherence to its security plan, address the need for changes to the approach to security in light of evolving circumstances and be carried out by individuals, independent of the area under review, who have the appropriate skills and experience.

7.3. Information Security Framework. Buyer highly recommends Supplier shall adopt and follow an industry recognized cybersecurity framework such as Health Information Trust Alliance ("HITRUST") framework; or, National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO) 27001. Each year, Supplier shall complete Buyer's vendor security assessment questionnaire and provide supporting documentary evidence. In the event, that there are security findings identified because of the Buyer's security assessment, Supplier shall agree to remediate the security findings within the Buyer's defined remediation timeframes. If Supplier fails to complete Buyer's vendor security assessment questionnaire and/or vendor security assessment remediation efforts in Buyer's sole opinion, Buyer may terminate any PA or SOW by giving Supplier fifteen (15) days' prior written notice.

7.3.1. Right to Conduct an On-Site Assessment. With reasonable notice and during normal business hours, Supplier agrees to allow Buyer, or its designated third party (under proper confidentiality obligations), to conduct an on-site assessment to ensure Supplier's compliance with the requirements of this document.

7.3.2. Regulatory Audits and Examinations. To the extent permitted by law, Supplier shall notify Buyer if a federal or state regulatory agency requests a review, audit or other examination of the services or records maintained by Supplier on behalf of Buyer. Supplier shall fully cooperate with Buyer and any regulator(s) in the event of an audit or review.

7.4. Identification of Risks Related to Third Parties. Supplier shall identify the risks to its information and information assets from business processes involving third parties and implement appropriate security controls. Supplier shall evaluate any information security risks posed by third parties prior to establishing a relationship with such third party. Once a relationship has been established, Supplier shall evaluate the third party's information systems on a scheduled ongoing basis.

7.4.1. Addressing Security in Third Party Agreements. Supplier shall maintain written agreements with its third parties that include an acknowledgement that such third parties are responsible for maintaining the security of the information. Supplier shall ensure that agreements with third parties cover all relevant information security requirements to the extent that the third parties are accessing, processing, or storing Buyer's data.

7.5. Evidence of Third-Party Risk Management Program. Supplier shall perform third party risk assessment for their Suppliers that access, process, and/or store Buyer's data. Supplier shall provide evidence of a third-party risk management program. Supplier agrees to provide evidence of a security assessment of any third parties that have access to Buyer's data.

8. Compliance

8.1. Identification of Applicable Legislation. Supplier shall explicitly define, document, and maintain all relevant statutory, regulatory, and contractual requirements for each information system type. The specific controls and individual responsibilities to meet these requirements shall be similarly defined and documented, and then communicated to the user community through a documented security training and awareness program.

8.2. Protection of Buyer Records. Supplier shall protect important records from loss, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements.

8.3. Regulation of Cryptographic Controls. Supplier shall use cryptographic controls in compliance with all relevant agreements, laws, and regulations. Supplier shall implement strong cryptographic controls for secure file transfers, data at rest and email communications, which may contain sensitive data. The compliance with all relevant regulations shall be reviewed at least on an annual basis.

8.4. Information Systems Audit Controls. Supplier shall develop audit requirements and activities involving checks on operational systems to minimize the risk of disruptions to business processes. An annual audit planning and scoping process shall exist and consider risk, involvement of technical and business staff, other ongoing projects and business impacts that may impact the effectiveness of the audit.

8.5. Payment Card Industry Information Security Standard Requirements. To the extent Supplier receives, accesses, or transmits cardholder data (e.g., credit or debit card data), Supplier acknowledges its responsibility to secure cardholder data and agrees to comply with applicable Payment Card Industry ("PCI") Data Security Standard ("DSS") requirements.

9. Asset Management

9.1. Inventory and Acceptable Use of Assets. Supplier shall identify and create an inventory of information assets. All information systems shall be documented and include rules for acceptable use and a method to accurately identify and assign ownership responsibilities to the appropriate users. The rules for

acceptable use shall be communicated to all information system users and describe their responsibilities and expected behaviors about information and information system usage.

9.2. Information Classification Guidelines. Supplier shall classify information based on its value, relevant legal requirements, sensitivity, and criticality to Supplier.

9.3. Information Labeling and Handling. Supplier shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification guidelines adopted by the Supplier. Sensitive information shall be physically and/or electronically labeled and handled appropriately regarding the level of risk the information or document. contains.

10. Physical and Environmental Security

10.1. Physical Security Perimeter. Supplier shall protect areas that contain information and information assets with physical security perimeters that include but are not limited to (barriers such as walls, card-controlled entry gates or manned reception desks). Information and information assets shall not be in areas that are unattended or have unrestricted access to the public.

10.2. Physical Entry Controls. Supplier shall protect secure areas with appropriate physical entry controls to ensure only authorized personnel are allowed access. Supplier shall maintain visitor access logs for facilities where information systems reside.

10.2.1. Working in Secure Areas. Supplier shall design and apply physical protections and guidelines for working in secure areas. The arrangements for working in secure areas shall include physical access controls for the employees, contractors, and third-party users.

10.2.2. Public Access Areas. Supplier shall control physical access points, such as delivery and loading areas and other points where unauthorized persons may enter the Supplier's premises, and, if possible, isolate access points from information processing facilities to avoid unauthorized access.

10.3. Securing Offices, Rooms, and Facilities. Supplier shall design and implement physical security controls for offices, rooms, and facilities to restrict access from the public.

10.4. Equipment Storage. Supplier shall store and protect equipment in a manner to reduce the exposure from environmental threats, hazards, and unauthorized access.

10.4.1. Supporting Utilities. Supplier shall protect equipment from power failures and other disruptions caused by failures in support utilities. Support utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning, shall be regularly inspected and tested to ensure their proper functioning and to reduce any risk of malfunction or failure.

10.5. Cabling Security. Supplier shall protect power and telecommunications cabling carrying data or supporting information services from interception or damage. Clearly identifiable cable and equipment markings shall be used to minimize handling errors, and access to patch panels and cable rooms shall be controlled.

10.6. Equipment Maintenance. Supplier shall maintain equipment to ensure its continued availability and integrity by developing and updating a, formal, documented information system maintenance policies, and procedures.

10.7. Secure Disposal or Re-Use of Equipment. Supplier shall ensure all items of equipment containing storage media that contain Buyer's data and licensed software have been removed or securely overwritten prior to disposal. Surplus equipment shall be stored securely while not in use. Devices containing Buyer's data shall be physically destroyed or the information shall be destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. A formal certificate of destruction is required to be provided by Supplier upon deletion of Buyer's data.

10.8. Removal of Property. Supplier shall ensure that equipment, information, or software shall not be taken off site without prior authorization and documentation. Employees, contractors, and third-party users who have authority to permit off-site removal of assets shall be clearly identified.

11. Communications and Operations Management

11.1. Documented Operations Procedures. Supplier shall formally document and maintain operating procedures and make them available to users on an as-needed basis. The documented procedures shall be prepared for system activities associated with information and communication assets.

11.2. Change Management. Supplier shall control and archive changes to information assets, systems, networks, and network services. Formal change management responsibilities and procedures shall be in place to ensure satisfactory control of all changes.

11.3. Segregation of Duties. Supplier shall enforce the separation of duties to reduce opportunities for unauthorized or unintentional modification or for misuse of Supplier's assets. No single user shall be able to access, modify or use assets without authorization or detection. Supplier shall identify duties that require separation and define information system access authorizations to support separation of duties.

11.4. Separation of Development, Test, and Operational Environments. Supplier shall separate and control development, test, and operational environments to reduce the risks of unauthorized access or changes to the operational system.

11.5. Monitoring and Review of Third-Party Services. Supplier shall regularly monitor and review the services, reports and records provided by third parties. Audits shall be carried out regularly to govern and maintain compliance with the product and/or service delivery requirements.

11.5.1. Managing Changes to Third Party Services. Supplier shall ensure that third parties use appropriate change management procedures for any changes to their provision of services or internal system. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls shall be managed, taking account of the criticality of business systems and processes involved and the reassessment of risks.

11.6. System Acceptance. Supplier shall establish acceptance criteria for new information systems, upgrades, and new versions. Suitable tests of the systems shall be carried out during development and prior to acceptance to maintain security. Supplier's management shall ensure that requirements for acceptance of new systems are clearly defined, agreed upon and documented.

11.7. Controls Against Malicious Code. Supplier shall implement detection, prevention, and recovery controls to protect against malicious code and provide appropriate user awareness procedures. Supplier shall document a formal policy and implement technologies , to ensure timely installations and upgrades for protective measures against malicious code is performed including the installation and regular automatic updating of anti-virus or anti-spyware software, including anti-virus definitions, and additional end point security controls should be implemented, such as windows firewall, and Data Loss Prevention ("DLP") solution, etc., and to be current whenever updates are available. Periodic reviews/scans shall be required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software.

11.8. Back-up. Supplier shall create and regularly test back-up copies of information and software and store them in a physically secure, remote location at a sufficient distance to make them reasonably immune from damage to data at the primary site. Supplier shall formally document backup processes for systems that process and/or store Buyer's data, which shall include the scope of data being imaged, frequency of imaging and duration of retention. This document shall be based on the contractual, legal, regulatory, and business requirements.

11.9. Network Controls. Supplier shall manage and control networks to protect Buyer data from threats and to maintain security for the network, including information in transit. Supplier shall implement controls to ensure the security of information in networks and the protection of connected services from unauthorized access. Controls shall be implemented to ensure the availability of network services and

information services using the network. Responsibilities and procedures shall be established for the management of equipment on the network, including equipment in user areas.

11.10. Management of Removable Media. Supplier shall document and implement formal procedures for the management of removable media. Media containing Buyer's data shall be physically stored, and its data shall be encrypted in accordance with the Supplier's data protection and privacy policy on the use of cryptographic controls until the media is destroyed or sanitized in accordance with the confidentiality and integrity requirements for its data classification level.

11.10.1. Physical Media in Transit. Supplier shall protect media containing information against unauthorized access, misuse, or corruption during transportation beyond Supplier's physical boundaries.

11.11. Exchange Agreements. Supplier shall establish and implement agreements for the exchange of information and software between Supplier and its third parties. The agreements shall specify the minimum set of controls on responsibility, procedures, technical standards, and solutions.

11.12. Audit Logging. Supplier shall maintain audit logs recording user activities, exceptions and information security events and maintain them for an agreed-upon period to assist in future investigations and access control monitoring. Retention for audit logs shall be specified by Supplier and retained accordingly.

11.13. Protection of Log Information. Supplier shall protect logging systems and log information against tampering and unauthorized access. Access to system audit tools and audit trails shall be limited to those with a job-related need.

11.14. Monitoring System Use. Supplier shall establish procedures for monitoring use of information processing systems and facilities to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed periodically. Supplier shall comply with all relevant legal requirements applicable to its monitoring activities. Items that shall be monitored include authorized access and unauthorized access attempts.

11.15. Clock Synchronization. Supplier shall ensure that the clocks of all relevant information processing systems within the Supplier's environment have been synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines.

12. Information Systems Acquisition, Development and Maintenance

12.1. Input Data Validation. Supplier shall apply checks to the input of business transactions, standing data, parameter tables and Buyer's data into applications and databases when system development is being performed to ensure that data is correct and appropriate.

12.2. Output Data Validation. Supplier shall validate data output from an application to ensure that the processing of stored information is correct and appropriate to the circumstances. Output validation shall be manually or automatically performed when system development on applications and database is being conducted.

12.3. Policy on the Use of Cryptographic Controls. Supplier shall develop and implement a policy on the use of cryptographic controls and support it with formal procedures. The cryptographic policy shall be aligned with the Supplier's data protection and privacy policy and shall address the use of encryption for protection of Buyer's data transported by mobile or removable media, devices or across communication lines.

12.4. Key Management. Supplier shall support the use of cryptographic techniques with the practice of key management. All cryptographic keys shall be protected against modification, loss, and destruction. Secret and private keys shall require protection against unauthorized disclosure, and all cryptographic keys shall be limited to the fewest number of custodians necessary. Equipment used to generate, store and archive keys shall be physically protected, and encryption keys shall be stored separately from encrypted data.

12.5. Protection of System Test Data. Supplier shall carefully select, protect, and control test data in non-production environments. The use of operational databases containing Buyer's data for non-production

purposes shall be avoided. If Buyer's data must be used for testing purposes, all sensitive information and content shall be removed or modified beyond recognition before use.

12.6. Access Control to Program Source Code. Supplier shall restrict access to program source code and associated items to prevent the introduction of unauthorized functionality and avoid unintentional changes.

12.7. Outsourced Software Development. Supplier shall supervise and monitor outsourced software development. Supplier shall have a contract for the outsourced development in place with the third party and address licensing arrangements, certification of the quality and accuracy of the work carried out, rights of access for audit of the quality and security functionality of code and escrow arrangements in the event of failure of the third party.

12.8. Control of Technical Vulnerabilities and Penetration Testing. Supplier shall perform vulnerability scans at intervals consistent to industry best practices to identify potential technical vulnerabilities based on notification of zero (0) day vulnerabilities. Supplier shall subscribe to industry recognized threat monitoring service. Once a potential technical vulnerability has been identified, Supplier shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls. Supplier shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required. Supplier shall agree in writing that prior to production the application will undergo a vulnerability and source code analysis. Postproduction, Supplier shall perform contractually agreed upon security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase. Upon request Supplier shall provide an executive summary report to Buyer of the results of the scans and tests along with a mitigation plan.

13. Information Security Incident Management

13.1. Reporting Information Security Incidents. Supplier shall report information security incidents through appropriate communication channels in accordance with mutual Agreements. All employees, contractors and third-party users shall be made aware of their responsibility to report any information security incidents as quickly as possible. Formal information security incidents reporting procedures to support Supplier's corporate policy shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security incident, treating the breach as discovered and the timelines of reporting and response. Supplier shall have a documented incident reporting standards for system administrators and other personnel to report anomalous events to the incident handling team in a timely manner, the mechanisms for such reporting and the information that should be included in the incident notification.

13.2. Responsibilities and Procedures. Supplier shall establish management responsibilities and procedures to ensure a quick, effective, and orderly response to Security Incidents.

13.3. Incident Response Plan. Supplier shall implement and maintain an existing incident response plan containing milestones and service level-agreements for its incident response capability, describing the structure and organization of the incident response capability, providing a high-level approach for how the incident response capability aligns with its overall organizational policies and procedures and meets the unique requirements of the Supplier, which relate to mission, size, structure and functions. The incident response plan will also define reportable incidents and resources needed to effectively maintain and mature an incident response capability, as well as provide metrics for measuring the incident response capability. The plan shall then be approved by designated Supplier officials.

13.3.1. Copies of the incident response plan shall be distributed to incident response personnel.

13.3.2. Reviews of the incident response plan shall occur annually and include a table-top exercise, documentation, test plan and results.

13.3.3. Revisions to the incident response plan shall be made to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

13.3.4. Supplier shall communicate incident response plan changes to incident response personnel.

13.4. Collection of Evidence. Supplier shall collect, retain, and present evidence after a Security Incident. The evidence that is collected, retained, and presented shall be done in accordance with the laws of the relevant jurisdiction(s).

14. Disaster Recovery Plan and Business Continuity Management

14.1. Including Information Security in the Disaster Recovery Plan and Business Continuity Management Process. Supplier shall develop and maintain a managed program and process to maintain or restore operations and ensure availability of information at the required level and in the required time frames following interruption to, or failure of, critical business processes for business continuity. Supplier shall maintain a single framework of business continuity plans to ensure all plans are consistent, to consistently address information security requirements and to identify priorities for testing and maintenance. The program and process shall identify all the assets involved in critical business practices, consider the purchase of suitable insurance, ensure the safety of personnel and the protection of information assets, formulate and document business continuity plans, and address information security requirements in line with the agreed upon business continuity strategy. Supplier must provide results of Business Continuity Planning ("BCP") sessions on an at least annual basis. BCP exercises must be conducted and reviewed with all downstream suppliers. Supplier will document BCP processes and procedures in support of products and services provided. This includes plans for the loss of critical resources including workplace, work force, third-party suppliers, and applications.

14.2. Testing, Maintaining and Re-Assessing Business Continuity Plans. Supplier shall test and annually update business continuity plans to ensure that they are up to date and effective. The business continuity plan tests shall ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

15. Cloud Security

15.1 Supplier shall establish a data protection agreement with third-party service provider such as a cloud service provider where Buyer data will be processed and/or stored.

15.2 Supplier shall monitor, review, and perform ~~a~~ security assessment on their cloud service provider(s) that will process and/or store any Buyer data. Upon request, Supplier shall provide Buyer with a copy of the assessment results.

15.3 Supplier shall maintain a complete inventory of cloud-based applications and/or systems in which Buyer data will be processed and/or stored.

15.4 Supplier shall ensure cloud service providers and/or any cloud-based solutions that are being utilized to deliver the services to the Buyer undergo ~~a~~ security assessment conducted by an independent third-party assessor to assess the security controls at least annually.

15.5 Supplier shall ensure access management controls are implemented in cloud-based environments and/or applications that will be utilized to process and/or store any of the Buyer's data. Access management controls shall include but are not limited to implementing multifactor authentication ("MFA"), performing periodic access reviews and ensuring minimum necessary access is granted to systems and applications in which Buyer data will be processed and/or stored.

15.5.a. If security responsibilities for cloud environments are shared between Supplier and Buyer, roles and responsibilities must be documented and communicated. Supplier must notify Buyer promptly of any personnel changes impacting such security responsibilities and operation for the cloud environment.

15.6 Supplier shall ensure Buyer data that will be stored in cloud-based applications and/or systems will be stored and transmitted utilizing industry standard level encryption algorithms such AES-256. Supplier shall establish an encryption key management policy and procedure for data stored in the cloud environment.

15.7 Supplier shall ensure security event log and monitoring alerts are implemented in cloud-based applications and/or systems in which Buyer data will be processed and/or stored. System and event logs are retained for a minimum period of one (1) year for cloud environments.

15.8 Supplier shall ensure Buyer's data is segregated in cloud-based systems and/or applications where technically feasible.

15.9 Supplier shall ensure cloud service provider stores Buyer's data within the U.S. jurisdiction and geographically distributed locations for primary and redundant data centers.

15.10 Supplier shall ensure cloud-service provider follows data retention requirements based on compliance and regulatory requirements.

15.11 Supplier shall ensure that the cloud-service provider has business continuity and disaster recovery plan in place in the cloud environment. Supplier shall ensure business continuity and disaster recovery plans are periodically tested to ensure plans are operating effectively.

15.12 Supplier shall ensure cloud service provider maintains an incident response plan and processes for incident escalation and reporting of security incidents to Supplier. Supplier shall follow Section 13 (Information Security Incident Management) of this document to review and address the incident reported by the cloud service provider appropriately.

Supplier agrees to comply with the above Information Security requirements in form and substance.

Signature: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 5

Supplier Software License
To be Added or Intentionally Omitted

EXHIBIT 6
Offshore Locations

Buyer approves of the use of the following offshore locations for Supplier services or resources set forth in the Master Statement of Work or Statement of Work. Complete each column for each offshore location.

Name of entity supplying offshore services Subsidiary/Affiliate/name or subcontractor	Specific offshore location address	General description of services	Will offshore location have access to PHI/PII (Yes or No)	Will offshore location be receiving and/or storing PHI/PII? (Yes or No)	Method of access or receipt of PHI/PII may include: VDI, VPN, email, excel, secure file transfer, etc. (Yes or No)

In the event of any offshore services or resources use remote locations other than listed above Supplier must provide the address of such remote location.

EXHIBIT 7
Service Level Agreement (SLA)
(Template for SOW/MSOW)

Definition	Measurement	Time Period	Penalty