PARTICIPATION AGREEMENT

BETWEEN [ENTITY] AND [SUPPLIER]

This Participation Agreement ("PA") 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 ("Enterprise MSA") (CID# XXXX) 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 1 - Statement of Work
b. Exhibit 2 – Consulting Services Role Descriptions
c. Exhibit 3 – Rate Schedule (For Time and Materials Only)
d. Exhibit 4 – Information Security Requirements
e. Exhibit 5 – Contingent Labor Requirements
f. Exhibit 6 – Supplier Software License (Supplier Paper to be Inserted)
g. Exhibit 7 – Change Request Form

2. **Term of Participation Agreement**

2.1. 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. 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 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 Agreement immediately if the Department of Health and Human Services ("HHS") finds that Supplier has failed to satisfactorily perform services as accordance with terms of this agreement or any SOW governed by this Agreement.

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 Agreement 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 (i) beneficial ownership of twenty percent (20%) or more of the outstanding voting securities of the Supplier or (ii) 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 SOWs. The termination of this PA will not affect any 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 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.

4. **Statements of Work**

4.1. Content. Assignments or services under this PA shall be set forth in a Statement of Work ("SOW"), in a format substantially similar to Exhibit 1 ("Services"). Buyer must agree in writing to the Services prior to Supplier's commencement of any work under a SOW. Each SOW shall identify all acceptance criteria, acceptance standards, timeframes and quality assurance testing, if any, applicable to the Services to be rendered thereunder, and shall also identify Buyer's Contract Administrator for said Services. Each SOW shall include the following items applicable to the work to be performed thereunder, unless otherwise mutually agreed in writing by the Parties: (i) the scope of the work to be performed, (ii) the key activities, (iii) the projected duration, (iv) the Deliverables (as defined below), Deliverables specifications, and due dates, (v) the roles and responsibilities of each of the Parties, (vi) any specific governance or resource management processes, reporting, and meeting requirements, (vii) a schedule of key personnel, (viii) any relevant assumptions, (ix) statement of the pricing arrangements, e.g., fixed rate, hourly, or not-to-exceed (if the SOW is an hourly rate project, provide an estimate of the number of hours necessary for the Services to be delivered under such SOW, (x) any applicable service level agreements, (xi) an estimate of expenses, and (xii) any other terms that specifically relate to the applicable Services or work under such SOW. Supplier shall provide the Services and produce the materials, works, or Deliverables (collectively, the "Deliverable(s)") as specified in the applicable SOW.

4.2. Change Requests. 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 a change to a SOW, and in advance of performing additional work, that Supplier considers a Buyer change request or series of requests to significantly increase the planned hours and/or costs for the required work. 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. The written authorization of the Contract Administrator and an amendment or change request to the SOW is required for any upward adjustment to pricing. If such authorization is not made, Supplier shall not be required to perform such additional services. Supplier has no authority to implement changes to any SOW without the Buyer Contract Administrator's written approval via an amendment to the SOW.

4.3. Entirety. This PA incorporates each SOW in its entirety. The parties agree that any 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 SOW expressly states otherwise.

5. **Government Programs**

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: https://www.bcbsm.com/suppliers/help/documents-forms.html , 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/suppliers/help/documents-forms.html (under "Government compliance"), 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. **Subcontracting**

Supplier shall not subcontract its obligations under this Agreement 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 Agreement in the same manner as Supplier.

8. **Intellectual Property**

8.1. Reporting of Work Product. For purposes of this Agreement, "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 Agreement, 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. **Offshoring**

Supplier shall not send an individual's protected health information as defined by the Health Insurance Portability and Accountability Act of 1996, as amended (PHI), or any individual's personally identifiable information (PII) to a location outside of the United States or allow access to PHI or PII from an offshore location without Buyer's prior written consent.

10. **Payment Terms**

Payment terms are 2% 15/Net 60. Payment for a properly submitted invoice is due within 60 days after Buyer receives the invoice. 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 Agreement, the following annual volume rebate shall apply:

11.2. If the YTD Contract Volume 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 the total amount of payments made and outstanding receivables due for that calendar year. Any and all amounts due to Buyer under this Section shall be paid in full by check within one hundred and twenty (120) days of the end of the just completed calendar year to: Blue Cross Blue Shield of Michigan, Attn: Accounts Payable, Mail Code 1011; 600 Lafayette East, Detroit, Michigan 48226 a copy of the annual volume discount check and/or credit statement shall be emailed to the Contract Administrator and the Procurement Representative.

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

11.6. Buyer is not required to purchase any specific volume of services from Supplier during the term of this Agreement.

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

12. **Diverse Supplier Requirement**

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 Agreement. 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 Agreement and can be located through the following hyperlink: https://www.unifiedtier2.com/request-reporting-access.html

13. **Non-Solicitation of Employees**

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.

14. **Notices**

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

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

SIGNATURE BLOCK APPEARS ON THE FOLLOWING PAGE

With a copy 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 Independent Contractor: Notices shall be sent to the address listed in the Recital section of this Agreement unless otherwise specified herein.

BLUE CROSS BLUE SHIELD OF MICHIGAN:

By: _____

Name:_____

Title: _____

Date: _____

By: _____

Name:_____

Title: _____

Date: _____

SUPPLIER:

By: _____

Name:_____

Title: _____

Date: _____

EXHIBIT 1
Statement of Work

BETWEEN

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

AND

SUPPLIER

This Statement of Work #_____ and any attachment(s) hereto ("SOW") is governed by the (insert Title of Master Agreement) (insert Master Contract ID #_____) between Blue Cross Blue Shield of Michigan ("Buyer") and (insert Supplier Name as listed on the Master Agreement) ("Supplier") effective (effective date of Master Agreement) ("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. (Contract Administrator to include a 2-3 of sentence summary of the SOW)

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

C. Scope of Work.

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

Supplier Services	Deliverables

Work Location. Work against this SOW shall be performed at the following location: ____

D. Warranty Terms. Supplier warrants that work against this SOW is warranted for _____ 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 _____ 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. Expenses. Travel and travel-related expenses against this SOW shall not exceed _____. Supplier shall only invoice Buyer for travel and travel-related expenses which have been authorized by the Buyer Contract Administrator in advance and in writing.

C. Total Amount of SOW. The total billable amount of this SOW is $___.

D. 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

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

B. Purchase Order Number. Buyer shall assign a Purchase Order number to this SOW for administrative and invoicing purposes. All Supplier invoices shall include the assigned Purchase Order number.

C. Invoices. Invoices against this SOW shall be emailed to: _____

IV. Supplier Attestation

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

1. Invoicing. If applicable, Buyer shall generate an electronic invoice via the Buyer Services Procurement for the actual hours entered and approved in Microsoft Project and/or Services Procurement time sheets on the tenth day following the preceding financial month based upon the Supplier's invoicing cycling date. Buyer shall approve and pay the invoice based on the established payment terms and the current calendar year invoicing schedule with Supplier. Supplier shall only enter time in Microsoft Project for actual hours worked.

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 Contract Administrator and an Amendment to this SOW.

Role	Hourly Rate
<<TITLE. EXAMPLE: Consultant, Advanced>>	$<<>>

3. Insert IT 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 the Buyer IT Resource Management Office via ISResourceRequests@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 (MSP 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.

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

BLUE CROSS BLUE SHIELD
OF MICHIGAN

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 for Time and Materials Only

Overview: Charges during the term of the controlling Agreement shall be set forth in the Rate Schedule, attached here as Exhibit 2. 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.

Supplier may propose an adjusted Rate Schedule to Buyer no more frequently than once per 12-month period. Supplier shall send notice to Buyer 's Corporate Contract Administrator at the address provided in the Agreement at least sixty (60) calendar days prior to the end of the effective 12-month period of Supplier's proposed adjusted Rate Schedule. Buyer shall negotiate and approve or reject Supplier's adjusted Rate Schedule within thirty (30) calendar days of receipt of Supplier's notice.

Rate Schedule: The Rates are applicable to each hour worked by Supplier's personnel at a designated Level and are set forth in the Rate Schedule below.

Level	Rates per Hour

Promotional Increases: No rate increases due to Supplier's organizational promotions may occur without the prior written approval of Buyer 's Contract Administrator. In the event that Supplier proposes a promotional rate increase, Supplier must provide written notice to Buyer and, absent Buyer 's Contract Administrator's written approval of the increase, Supplier shall be obligated to replace the Supplier personnel with an alternate resource at the rate that was charged before that individual rate was increased. If any Supplier personnel is replaced during the term of any Statement of Work due to the operation of this section, Supplier and Buyer 's Contract Administrator shall agree on the duration of the training period to transition the new resource on to the Project, which shall be at no cost to Buyer.

IT Security Requirements

1. Purpose

1.1. This Supplier Privacy and 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"). All capitalized terms not defined herein shall have the meanings set forth in the Enterprise MSA – Standard Terms and Conditions, Participation Agreement, or Business Associate Agreement, as applicable.

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 management.

2.3. Buyer shall have the right to assess 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 are 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 and updated at least annually.

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

3.2.1. User Registration. Supplier shall implement and document a user registration and deregistration 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 identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identify of the user. Authentication and authorization mechanisms shall be applied for users and equipment.

3.2.3. 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 on a need-to-use basis and on an event-by-event basis in line with the access control policy.

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 only be accessed by authorized accounts, limit the number of unsuccessful log-on attempts , enforce recording of unsuccessful attempts, force time delay before further log-on attempts are allowed or reject any further attempts without specific authorization from an administrator, and 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, or not they are permitted to connect to the Supplier's network.

3.4.2. Remote Diagnostic & Configuration Port-Protection. Supplier shall control the physical and logical access to diagnostic and configuration ports. Controls for the access to diagnostic and configuration ports shall include the use of a key lock. 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. Buyer shall have the right to review the information system within every three hundred sixty-five (365) days to identify and disable unnecessary and non-secure functions, ports, protocols, and/or services.

3.4.3. Segregation in Networks. Groups of information services, users, and information systems shall be segregated on networks. Security gateways shall be used between internal network, external networks, 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 concerning information security 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, 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 sanctions 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, contract or agreement, or adjusted upon a change of employment. Changes of employment or other workforce arrangement shall be reflected in removal of all access rights that were not approved 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 physical and environmental hazards.

5.2. Risk Assessments. Supplier shall perform risk assessments to identify and quantify information security risks to Buyer. Supplier shall account for risks from sources including prior incidents experienced, changes in the environment, and any supervisory guidance. Risk assessments are to be performed at least annually, or when major changes occur in the environment, and the results reviewed annually.

6. Information Security Policy

6.1. Information Security Policy. Supplier shall develop, publish, and implement information security policy documents. The information security policy shall state the purpose and scope of the policy, communicate management's commitment, describe management’s and workforce member's roles and responsibilities, and establish Supplier's approach to managing information security. The documents shall be reviewed at planned intervals or if significant changes occur to ensure the policies' adequacy and effectiveness.

7. Organization of Information Security

7.1. Confidentiality Agreements. Supplier shall identify the requirements for confidentiality or non-disclosure agreements that reflect the Buyer's needs for the protection of information. These agreements shall be applicable to all personnel accessing covered information and shall comply with all applicable laws and regulations for the jurisdiction to which it applies. The requirements for confidentiality and non-disclosure agreements shall be reviewed at a planned interval and when changes occur that influence these requirements.

7.2. Independent Review of Information Security. Supplier shall review at least annually, or 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 strongly encourages and highly recommends Vendor (a) obtain within 2 years from the Effective Date, and maintain thereafter, a Health Information Trust Alliance (“HITRUST”) certification; or, (b) promptly adopt and follow an alternative leading, industry recognized cyber security framework, e.g., National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO) 27001. Each year, Supplier shall either provide a HITRUST certification that covers the scope of services being provided to Buyer or complete Buyer’s vendor security assessment questionnaire. If Vendor

fails to obtain or maintain a HITRUST certification or is unable to satisfy Buyer's vendor security assessment in Buyer's sole opinion, Buyer may terminate any PA or SOW by giving Vendor fifteen (15) days' prior written notice.

7.3.1. Right to Conduct an On-Site Assessment. With reasonable notice and during usual 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 then 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 ensure that agreements with third parties involving accessing, processing, communicating or managing its information or information assets, or adding products or services to information assets cover all relevant security requirements. Supplier shall identify and mandate information security controls to specifically address third party access to its information assets. Supplier shall maintain written agreements with its third parties that include an acknowledgement that such third parties are responsible for the security of the information.

7.5. Evidence of Third-Party Risk Management Program. For Suppliers that maintain or retain data and provide access to any third party, Supplier shall provide evidence of a third-party risk management program. Upon request from Buyer, Supplier agrees to provide evidence of an 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. The compliance with all relevant regulations shall be reviewed at minimum 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 Information Security Standard requirements.

9. Asset Management

9.1. Inventory and Acceptable Use of Assets. Supplier shall identify and create an inventory of assets and information. All information systems shall be documented and include rules for acceptable use and a method to accurately identify and assign ownership responsibilities to the proper individuals. The rules for acceptable use shall be communicated to all information system users and describe their responsibilities and expected behavior with regard to information and information system usage.

9.2. Classification Guidelines. Supplier shall classify information based on its value, relevant legal requirements, sensitivity, and its criticality to Supplier so that limitations can be put on the data internally and externally. Appropriate procedures for information labeling and handling shall be developed based on the classification system adopted by the 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 scheme adopted by 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 security perimeters (barriers such as walls, card-controlled entry gates, or manned reception desks). These areas shall not be located in areas that are unattended or have unrestricted access by the public.

10.2. Physical Entry Controls. Supplier shall protect secure areas with appropriate 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 protection and guidelines for working in secure areas. The arrangements for working in secure areas shall include controls for the employees, contractors, and third-party users.

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

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

10.4. Equipment Siting. Supplier shall site or protect equipment to reduce the risks from environmental threats and hazards and opportunities for 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 from their 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 correctly maintain equipment to ensure its continued availability and integrity by developing, communicating, and reviewing/updating a formal, documented information system maintenance policy and procedures.

10.7. Secure Disposal or Re-Use of Equipment. Supplier shall check all items of equipment containing storage media to ensure that covered information and licensed software has been removed or securely overwritten prior to disposal. Surplus equipment shall be stored securely while not in use. Devices containing covered information 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.

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 all users who need them. 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 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 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 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. 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 also provide appropriate user awareness procedures. Formal policies shall be required, and technologies implemented for the timely installation and upgrade of the protective measures, including the installation and regular, automatic updating of anti-virus or anti-spyware software, including anti-virus definitions, 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. A formal definition of the level of back-up required for each system shall be defined and documented including 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 in order to protect Buyer 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 covered information shall be physically stored and its data 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, and commensurate 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 produce audit logs recording user activities, exceptions, and information security events and keep them for an agreed 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 result 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 covered information 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 covered information 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 covered information for non-production purposes shall be avoided. If covered, or otherwise sensitive, information must be used for testing purposes, all sensitive details 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 take timely action in response to the identification of potential technical vulnerabilities. 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 penetration test. 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. Supplier shall provide written documentation to Buyer of the results of the scans and tests along with a mitigation plan. Supplier shall agree in writing that these vulnerabilities shall be mitigated within a pre-negotiated period.

13. Information Security Incident Management

13.1. Reporting Information Security Incidents. Supplier shall report Security Incidents through appropriate communications channels in accordance with the Enterprise MSA, Participation Agreement or Business Associate Agreement, as applicable. All employees, contractors, and third-party users shall be made aware of their responsibility to report any Security Incidents as quickly as possible. Formal 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 a Security Incident, treating the breach as discovered, and the timelines of reporting and response. Supplier standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of 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 develop an incident response plan containing a roadmap for implementing 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 and Supplier organization elements.

13.3.2. Reviews of the incident response plan shall occur annually.

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 and organizational elements.

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. Business Continuity Management

14.1. Including Information Security in the 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 scales, 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.

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.

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

Signature: _____

Name: _____

Title: _____

Date: _____

Exhibit 5
Contingent Labor Requirements

INTENIONALLY OMITTED

Exhibit 6
Supplier Software License

INTENTIONALLY OMITTED

Exhibit 7
Change Request Form

INTENTIONALLY OMITTED