UNIVERSAL MASTER SERVICES AGREEMENT

This Universal Master Services Agreement ("UMSA" or "Agreement"), Contract ID #XXXXX, is between Blue Cross Blue Shield of Michigan Mutual Insurance Company, with its principal place of business, 600 Lafayette East, Detroit, MI 48226 (and its affiliate, insert Name and Principal Office Address) ("Buyer" OR "collectively referred to as "Buyer") and Supplier Name, a Jurisdiction e.g., Michigan or State Name Corporation or Limited Liability Company, whose principal place of business is Supplier's Principal Office Address ("Supplier").

KEEP LANGUAGE BELOW IF THE CURRENT MSA OR AN EMSA/PA IS THE GOVERNING AGREEMENT AND IS BEING REPLACED WITH THIS NEW AGREEMENT OR DELETE IF NEW SUPPLIER

A (Master Service Agreement or Enterprise Master Services Agreement and Participation Agreement, Contract ID #XXXX), ("MSA" or "EMSA" or "PA) (was/were)) previously executed between Buyer and Supplier. Upon full execution of this Agreement, the (MSA, EMSA/PA) shall no longer be valid and any active statements of work formerly governed by the (MSA/ EMSA and PA) shall be governed by this UMSA.

1. **Agreement Exhibits:**

   1.1 Exhibit 1: Information Security Requirements
   1.2 Exhibit 2: Supplier Software License (Add or Intentionally Omit)
   1.3 Exhibit 3: Offshore Locations

2. **Term**

   2.1 Term. This Agreement shall become effective on EFFECTIVE DATE ("Effective Date") and shall end on EXPIRATION DATE ("Term").

3. **Statements of Work and Services**

   3.1 Services. Assignments, tasks, products, functions or services provided by Supplier under this Agreement ("Services") shall be set forth in a Statement of Work or other mutually agreed contract document ("SOW") in a format substantially similar to the template found at https://www.bcbsm.com/suppliers/help/documents-forms.html. Supplier is a non-exclusive provider of the Services to Buyer, and Buyer may obtain similar services from other third parties.

   3.2 Changes. Supplier shall obtain Buyer's written approval prior to any changes to the Services.

   3.3 Service Levels and Remedies. Supplier shall adhere to the service levels set forth in the SOW. In the event of Supplier's failure to meet the agreed upon service levels, Buyer shall be entitled to remedies as outlined in the SOW, including but not limited to service credits. Any service credits granted pursuant to this Section 3.3 shall be applied to future invoices or refunded to Buyer. Repeated failures to meet service levels shall be subject to termination pursuant to Section 8.2 of this Agreement.

   3.4 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.

3.5 Entirety/Amendments. This Agreement incorporates each SOW in its entirety. The parties agree that any SOW provision that is inconsistent with this Agreement shall be of no force or effect, shall be disregarded and this Agreement shall take precedence, unless the SOW expressly states otherwise. In order for a SOW to modify or amend this Agreement with respect to a particular SOW, the modifying or amending term must be included within the "Override" section of the SOW and must list the specific term from this Agreement that it overrides. Any such modifying or amending terms shall apply only to the SOW in which such deviations are contained.

4. Expenses

4.1 Supplier shall not be reimbursed for expenses under this Agreement except as approved by Buyer in the applicable SOW.

5. Invoicing

5.1 All invoices shall be submitted monthly through the Oracle Supplier Portal, unless otherwise stated in the SOW payment schedule. All invoices shall contain separate invoice numbers. All invoices shall have Buyer's purchase order number printed at the top and be itemized with only Buyer approved expenses incurred during the billing period. If invoices are submitted without the proper purchase order number printed on the invoice, that invoice shall be considered improperly submitted and Buyer may reject such invoice upon which Supplier shall then be obligated to resubmit the invoice pursuant to Buyer's requirements.

5.2 In the event Buyer issues a work order and/or a purchase order, Supplier shall generate an electronic invoice and submit it through the Oracle Supplier Portal.

5.3 Expense receipts, or copies of expense of receipts, shall be attached and made part of submitted invoices for billable expenses approved in the SOW. Supplier shall submit one invoice per SOW per calendar month, or as otherwise agreed upon in the SOW, against the Buyer's purchase order through the Oracle Supplier Portal. If requested, Supplier shall promptly provide reasonably detailed information on fees and expenses sufficient to answer any Buyer concerns or questions pertaining to its payment obligations within ten (10) business days. Buyer shall not delay payment for invoice items not in dispute. Payment on questioned items may be delayed until after receipt of such information and resolution of any concerns or questions and shall not be considered a default in Buyer's payment obligations.

5.4 A purchase order number shall be provided by Buyer for each SOW or agreement for the purchase and/or license of products and/or provision of services that is executed between the parties for administrative and invoicing purposes.

6. Payment Terms

6.1 Payment terms are 2% 15/Net 60. Payment is due within sixty (60) days of receipt of a properly submitted invoice in the Oracle Supplier Portal and Buyer approval. In the event Buyer makes payment on or before the 15th day of 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 Buyer transfers the invoice payment via electronic transfer method

(e.g., EFT) or the date on any other payment instrument. In no event shall Buyer be liable to Supplier for any interest or late payment fees. All agreed upon fees in the applicable SOW are final upon execution.

7. Annual Volume Discount

7.1 During the term of this Agreement, the following annual volume rebate shall apply:

7.2 If the YTD Contract Volume, defined below in subsection 7.4, 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%.

7.3 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).

7.4 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.

7.5 In the event Buyer is owed any amounts under this Section after the termination 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.

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

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

8. Termination

8.1 Termination for Convenience. Buyer, but not Supplier, may terminate this Agreement, any SOW, or any signed document governed by this Agreement, in whole or in part, for its sole convenience upon thirty (30) days' prior written notice. Supplier shall be paid for Services 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.

8.2 Termination for Cause. Buyer shall have the right to terminate this Agreement, any SOW, or any signed document governed by this Agreement, immediately, in whole or in part, and at no cost or charge, upon written notice in the event of Supplier's material breach of this

Agreement. Supplier shall be paid for Services 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.

8.3 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 breached this agreement or failed to satisfactorily perform Services in accordance with terms of this Agreement or any SOW governed by this Agreement.

8.4 Termination for Change 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 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.

8.5 Termination Effect on SOW. The termination of this Agreement will not affect any SOW that, by its own terms, extends beyond the effective date of termination of this Agreement, and the parties will be bound by the terms of this Agreement until termination or expiration any SOW governed by this Agreement. The expiration or earlier termination of this Agreement 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 Agreement. Termination of this Agreement will be in addition to and not in lieu of any other remedies available to a party in law or in equity.

8.6 Continued Performance. Each party agrees to continue performing its obligations under this Agreement while any dispute is being resolved, except to the extent the issue in dispute precludes performance (dispute over payment in good faith shall not be deemed to preclude performance).

8.7 Transition Assistance. Upon expiration or termination of this Agreement for any reason, Supplier will, at Buyer's request, provide transition assistance services and perform its obligations under this Agreement on the same terms and conditions and at the then-current rates immediately prior to the date of expiration or termination. Such transition assistance services will allow Buyer to achieve an orderly transition and such period will not exceed one hundred twenty (120) calendar days, (the "Transition Period").

8.7(a) Divestiture. If Buyer provides Supplier written notice that it has divested an affiliated entity receiving services under this Agreement, Supplier agrees that it will continue to perform its obligations for such divested affiliated entity until the earlier of ninety (90) days after the

divestiture closing date or the execution of a new agreement between the divested affiliated entity and Supplier.

9. Compliance with Law

9.1 Both parties will comply with all federal, state, and local laws, ordinances, rules, and regulations applicable to its activities and obligations under this Agreement. Supplier warrants and represents that it has all legally required licenses and permits needed to perform the services ("Services") and shall provide copies of such licenses and permits to Buyer upon request. Additionally, if applicable, Supplier specifically agrees to comply with 45 CFR 156.340.

9.2 Retention of Records & Data: Supplier shall maintain books, records, documents, and other evidence pertaining to this Agreement and any SOW, to the extent and in such detail shall adequately reflect the Supplier's performance. Supplier shall retain such records for a period of six (6) years following the later of: (a) expiration or termination of this Agreement, including any active SOWs; or (b) Buyer's final payment; provided that if the Services pertain to Buyer's Medicare business, then such records shall be retained for a period of ten (10) years following the later of: (i) expiration or termination of this Agreement and applicable SOW; or (ii) Buyer's final payment. When a record or information completes its retention period, Supplier shall delete or dispose of such information in accordance with its obligations in Section 11.3.

10. Audit

10.1 With at least thirty (30) days written notice to Supplier and during usual business hours, Supplier shall allow Buyer, or its designated third party (under confidentiality provisions no less stringent than those set forth herein) to audit relevant facilities, systems, business record policies, procedures, internal practices, books, system procedures and records, and data logs of Supplier and/or its subcontractors, as necessary to ensure compliance with this Agreement and any applicable federal and state laws, and to verify that Supplier's invoices were true and correct for time, travel, or other expenses billed to Buyer. Compliance includes, but is not limited to, ensuring that adequate HIPAA related privacy and security standards, including appropriate administrative, technical, and physical safeguards have been identified, and are implemented by Supplier to prevent the unauthorized disclosure of Protected Health Information. Supplier shall cooperate with Buyer in all reasonable respects in connection with such audits and shall be limited to not more than once in a twelve (12) month period except in the case of security incidents or risks identified in audit findings. Supplier or its authorized personnel shall assist Buyer's access to its systems, including any system with Buyer data. If applicable, Supplier and/or its subcontractors will permit access by the Secretary of HHS and the Office of the Inspector General ("OIG") or their designees in connection with their right to evaluate through audit, inspection, or other means, to the Supplier's books, contracts, computers or other electronic systems records, including medical records and documentation, relating to Supplier's or Buyer's obligations in accordance with Federal standards until ten (10) years from the termination date of this Agreement.

10.2 Certifications: If Supplier has performed an SSAE 18 SOC1 Type II or SOC 2 Type II certification (or comparable certifications such as HITRUST or ISO 27001) then Supplier shall provide Buyer with copies of such certification reports upon Buyer's request.

11. Confidentiality

11.1 "Confidential Information" means (i) any written or oral information furnished by, made available directly or indirectly by, or obtained from one party from the other, which a reasonable person would determine should be treated as confidential, (ii) any information concerning the operations, affairs and businesses of Buyer, its customers, or clients, and (iii) all information, including but not limited to the terms and conditions of this Agreement, trade secrets, and proprietary information, made known to any party to this Agreement shall be considered "Confidential Information." During the term of this Agreement and thereafter, all Confidential Information disclosed by either party shall remain the disclosing party's property.

11.2 The parties agree that Confidential Information shall remain confidential and may be further disclosed only with written consent from the disclosing party. The parties agree that this provision shall not limit or restrict Buyer from sharing Confidential Information with its affiliates or subsidiaries. The parties agree that this provision shall not limit or restrict Buyer from sharing Confidential Information in furtherance of its business objectives with employees, contractors, or consultants, provided that such employees, contractors, or consultants are under confidentiality obligations at least as stringent as those set forth herein.

11.3 At the conclusion of the Term or as required due to any retention obligations, or upon written request, all files containing Confidential Information shall be promptly returned to the disclosing party, or at the disclosing party's sole discretion, erased or rendered permanently inaccessible. Upon the disclosing party's request, the receiving party shall deliver a written statement that a diligent search and inquiry has been made for any Confidential Information, and that all such Confidential Information was returned, erased, or rendered permanently inaccessible. Neither party may keep or use any Confidential Information after the engagement is completed, except to the extent required by law, or for archival purposes only subject to the terms and conditions of this Agreement.

11.4 Except as set forth in the business associate agreement ("BAA") between the parties, if any, in the event of any actual or suspected misuse, disclosure or loss of, or inability to account for, any Confidential Information of the furnishing party, the receiving party promptly (within at least twenty-four (24) hours) shall: (i) notify the furnishing party; (ii) furnish the other party full details of such, and use reasonable efforts to assist the other party in investigating; and (iii) cooperate with the furnishing party to halt any continuing breach and/or disclosure of such Confidential Information.

11.5 Notwithstanding anything to the contrary contained herein, the provisions of this Section shall not apply to any information which: (i) at the time disclosed or obtained is in the public domain; (ii) becomes part of the public domain through no fault of the receiving party; (iii) was communicated by a third party who is not, to the receiving party's knowledge, subject to any

confidentiality obligations with respect thereto; (iv) is independently developed by the receiving party; or (v) is required to be disclosed by operation of law.

12. Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

12.1 Business Associate. If the Services qualify Supplier as a "Business Associate" of the Buyer under HIPAA, then Supplier shall sign a separate BAA with Buyer that provides all the protections required by HIPAA. The terms and conditions and obligations of Supplier under the BAA are incorporated into this Agreement where Supplier acts in the capacity as the Buyer's Business Associate.

13. Insurance

13.1 Supplier shall maintain the following insurance policies with minimum limits as specified below and with insurance companies authorized to do business in the State of Michigan with a minimum AM Best rating of A-.

13.2 Coverage Type & Limit Amount Table:

Coverage Type	**Limit Amount**
Worker's Compensation Insurance – if supplier is statutorily required to maintain such coverage	Statutory amounts
Workers Compensation Employer's Liability	$1,000,000 Each Accident $1,000,000 Disease -- Each Employee $1,000,000 Disease -- Policy Limit
Commercial Automobile Liability - Bodily Injury and Property Damage Combined - Owned (if supplier owns automobiles in the United States) - Non-owned and Hired Cars (if Supplier travels to or maintains operations in the United States)	$1,000,000 -- Combined Single Limit Each Accident
Commercial General Liability - Bodily Injury and Property Damage - Premises/Operations - Products/Completed Operations - Personal and Advertising Injury - Contractual Liability	$1,000,000 –Each Occurrence
Foreign (if offshore services are in scope) - General Liability including Products Liability - Foreign Voluntary Workers Compensation Employers Liability - Contingent Automobile Liability	 $1,000,000 – Each Occurrence Country of Origin/Hire Benefits $1,000,000 Each Accident $1,000,000 Disease – Each Employee $1,000,000 Disease –Policy Limit $1,000,000
Excess/Umbrella/ Liability Insurance	$4,000,000 -- Each Occurrence/Aggregate
Privacy and Network Security Liability - Worldwide Territory subject to applicable trade and economic sanctions or where prohibited by law - Credit Monitoring & Notification - Privacy Liability	$5,000,000 -- Per Claim/Aggregate

- Crisis Management Coverage - Wrongful Disclosure of Data - Disclosure of HIPAA protected health information	
Professional Liability Errors & Omissions - Worldwide Territory subject to applicable trade and economic sanctions or where prohibited by law	$1,000,000 -- Per Claim/$3,000,000 Aggregate

13.3 Supplier's liability is not limited by the amount of insurance stated above.

13.4 Offshore Subsidiaries, Affiliates and Subcontractors of Supplier shall maintain insurance coverages and limits that comply with all local compulsory and non-admitted insurance regulations in the applicable territories.

13.5 Supplier shall name Buyer (including its affiliates for whom Services are provided hereunder) as additional insured(s) on its Automobile, Commercial General Liability, Foreign and Umbrella policies and such insurance shall state that it is primary and noncontributory with respect to any insurance coverage carried by Buyer.

13.6 Workers' Compensation coverage shall provide a waiver of subrogation against Buyer.

13.7 Certificates of insurance evidencing insurance coverages shall be furnished to Buyer prior to commencement of work. All insurance coverages and limits noted herein must maintained while this Agreement is in force. Such evidence and notices shall be updated annually and as otherwise requested from time to time by Buyer.

13.8 If any of Supplier's insurance policies are written on a claims-made basis, then Supplier shall maintain such claims-made coverage with the same policy limits for the term of the Agreement and following the termination date for a period of three (3) years. This requirement may be fulfilled by the acquisition of tail insurance coverage.

14. Indemnification

14.1 Each party (the “Indemnifying Party”) shall indemnify, hold harmless, and defend the other party and its officers, directors, shareholders, employees, agents, affiliates, successors, and permitted assigns (collectively, the “Indemnified Party”) against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorney fees (collectively, “Losses”), relating to, arising out of, or resulting from any third-party claim (“Claim”) alleging (i) breach of any representation, warranty, or covenant under this Agreement by the Indemnifying Party; (ii) any negligent (or more culpable) act or omission of the Indemnifying Party (including any recklessness or willful misconduct) in connection with the performance of its obligations under this Agreement; or (iii) any bodily injury, death of any person, or damage to real or tangible personal property caused by the negligent acts or omissions of the Indemnifying Party.

14.2 Process. The obligations under this Section 14 are conditioned upon the following: (i) the indemnified party first providing written notice of the Claim to the indemnifying party promptly

after the indemnified party becomes aware of or reasonably should have been aware of the Claim (provided, however, the failure to provide such notice will only relieve the indemnifying party of its indemnity obligations hereunder to the extent prejudiced thereby); (ii) indemnified party tendering sole and exclusive control of the Claim to the indemnifying party at the time the indemnified party provides written notice of such Claim; and (iii) the indemnified party providing reasonable assistance, cooperation and required information with respect to defense and/or settlement of the Claim, including providing the indemnifying party with access to documents and personnel at the indemnifying party's request and expense. The indemnified party may at its sole expense participate in the Claim. The indemnifying party shall not agree to any settlement of a Claim that includes an injunction against the indemnified party or admits liability without the indemnified party's prior written consent.

15. Government Programs

15.1 Supplier agrees to comply with the Government Programs provisions applicable to Supplier, as revised from time to time. The current versions of the Government Programs provisions can be found by visiting the policies found at the following link and incorporated herein by reference. https://www.bcbsm.com/suppliers/help/documents-forms.html. Buyer shall provide Supplier written notice of any revision thereto, and the revised version shall replace and supersede any and all prior versions.

16. Federal Employee Program and E-Verify

16.1 Supplier agrees to comply with the Federal Employee Program Addendum ("FEP Addendum") as revised from time to time, as applicable to Supplier. The current version thereof can be found by visiting the following site which is incorporated herein by reference: Federal Employee Health Benefits Program Addendum.

16.2 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.

16.3 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.

17. Supplier Personnel and Subcontracting

17.1 Supplier shall utilize, to perform the Services, employees and Subcontractors (subject to Section 19.2 below) (collectively, "Supplier Personnel") who are properly educated, trained, experienced, and fully qualified for the Services they are to perform. 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 18 (Intellectual Property) below. Supplier is fully and unconditionally responsible for all Supplier Personnel compliance with this Agreement, including any applicable SOW.

17.2 Supplier shall not subcontract its obligations under this Agreement to any third-party company, individual or Supplier affiliate (collectively, "Subcontractor") unless Supplier

provides Buyer with written notice and Buyer subsequently provides written approval of such Subcontractors, the decision of which shall be in Buyer's sole discretion. Supplier agrees that (a) any Subcontractor shall comply with all terms and conditions of this Agreement in the same manner as Supplier, including all applicable accreditation standards, and federal, state, and regulatory standards; and (b) Supplier remains fully and unconditionally responsible for all Services and for the Subcontractors' compliance with this Agreement, including any applicable SOW.

18. Offshore

18.1 Supplier and any approved Subcontractor shall not provide any services or support of such services outside of the United States and its territories 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 and its territories.

18.2 If Supplier desires to access, store, host, view, transfer, or exchange PHI/PII, Confidential information or financial data pursuant to the Services or support of such services outside the United States and its territories, Supplier shall complete an Offshore Vendor Form, located at https://www.bcbsm.com/suppliers/help/documents-forms.html, and the Offshore Locations Form, located in Exhibit 3, and submit to Buyer. If Buyer consents to receive offshore services, such consent will be documented within Exhibit 3 or a SOW and shall be limited in scope to those services set forth in the Offshore Vendor Form accepted by Buyer. If Supplier desires to modify any offshore locations, Supplier shall notify Buyer in writing and submit a new Offshore Vendor Form and Offshore Locations Form for Buyer's approval.

19. Intellectual Property

19.1 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 Agreement. Supplier shall promptly disclose all Work Product to Buyer upon its development, invention, discovery, creation, authoring or origination.

19.2 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.

19.3 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.

19.4 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

Supplier 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 to Buyer.

19.5 Supplier Materials. To the extent that the Work Product includes Supplier's materials or materials of Supplier's licensors ("Supplier 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 Supplier Materials, including all such modifications, improvements and derivative works thereof, solely to the extent such Supplier 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 Supplier Materials in any Work Product without prior written permission of Buyer.

19.6 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 Agreement shall be and shall remain the property of Buyer, whether, or not registered.

19.7 Open-Source Software. Supplier represents and warrants, and shall ensure that its Personnel warrant, that it will not supply to Buyer any Work Product that is based upon, incorporates, links to or otherwise relies on software code that is subject to an "open source" license, including without limitation the GNU General Public License or other licenses listed at www.opensource.org without Buyer's prior written consent. Open Source Code means program code and related materials that are certified as open source by Open Source Initiative or a similar organization (and its successors) or code that is available to the general public for use or modification free of charge. ("Open Source Software") Such consent may be granted or withheld in Buyer's sole and exclusive discretion and must include a separate indication of approval by Buyer's legal counsel.

19.8 Third-Party Software. If Supplier intends to develop a deliverable in a manner that incorporates or requires Buyer to use any Third Party Materials in order to use such deliverable, then Supplier will (i) provide Buyer with prior notice, specifying in reasonable detail the nature of the deliverable's dependency on or use of the Third Party Materials, and (ii) provide Buyer with (for no additional cost or on such terms as may be acceptable to Buyer) a perpetual, irrevocable, royalty-free, non-exclusive right and license for Buyer to use the Third Party Materials in connection with the use of the deliverable. "Third Party Materials" shall mean data, images, programming, computer code, graphics, text, or other materials made, conceived, or developed by third parties, other than Open-Source Software described in

Section 5.7 above, that will be incorporated into the Deliverable(s) or used to make the Deliverables useful to Buyer.

19.9 No Malicious Code. Supplier represents and warrants that: (i) any Deliverables provided by Supplier, or its Personnel under this Agreement will not, at the time of installation, contain any Disabling Code; and (ii) Supplier and its Personnel shall not at any time intentionally or negligently introduce any Disabling Code to any of Buyer's or its customers' systems or to the Deliverables or any Work Product. In the event Supplier breaches this warranty, Supplier shall, at Buyer's option and in addition to such other rights as Buyer may have with respect thereto, take all steps necessary at Supplier's sole cost to remove the Disabling Code and assist Buyer at no additional charge in restoring any and all data or programming lost by Buyer or its customers, or the end users of either of them, as a result of such Disabling Code. "Disabling Code" shall mean any virus, worm, trap door, back door, timer, clock, counter or other code, limiting routine, instruction or design that would erase data or programming or otherwise cause its software to become inoperable or incapable of being used in the full manner for which it was designed and created, or which permit unauthorized access to the system or unauthorized changes to the software, its functionality, or its output. Disabling Code shall include, without limitation, any limitations that are triggered by: (a) the software being used or copied a certain number of times, or after the lapse of a certain period of time; (b) the software being installed on or moved to a central processing unit or system different from the central processing unit or system on which the software was originally installed; or (c) the occurrence or lapse of any similar triggering factor or event.

19.10 Survival. The obligations of this Section shall survive the termination or expiration of this Agreement.

20. Representations and Warranties

20.1 Supplier Services Warranty. Supplier represents and warrants for twelve (12) months after receipt of final payment (i) the Services will be performed in a good and workmanlike manner, (ii) the Services will be performed by qualified personnel using reasonable diligence and care, and (iii) any Supplier applications will be performed substantially in accordance with their intended purpose and documentation.

20.2 Mutual Representations. Each party represents to the other that (i) it has duly formed and in good standing, (ii) it has the requisite power and has taken all actions necessary to execute this Agreement and all SOWs; and (iii) this Agreement and each SOW when signed by each party shall constitute legal, valid and binding obligations of that party in accordance with its terms.

21. Electronic Accessibility Compliance

21.1 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 Sections 504 and/or 508 of the Rehabilitation Act. Content must also meet the most current Web Content Accessibility Guidelines (“WCAG”) 2 requirements.

22. Non-Solicitation of Employees

22.1 With the exception of generalized recruiting practices, including but not limited to responses to advertisements, internet postings and job fairs, should either party desire 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 meetings as required.

23. Operational Matters

23.1 Removal of Supplier Personnel Performing Services. If applicable, Buyer in its sole discretion may request the removal of any individual that Supplier has assigned to perform the Services. After Buyer notifies Supplier in writing, Supplier shall immediately cease scheduling the individual to provide or support Services to Buyer.

23.2 Property Rules. On-site Supplier Personnel shall follow and adhere to the Buyer policies and procedures outlined on Buyer's Supplier Online Portal including, by way of example only and without limitation, (a) sign-in procedures, (b) identification badges, (c) executing confidentiality statements, (d) participation in any required training, or (e) Buyer's parking regulations.

23.3 Former Employees. If Supplier plans to assign a former Buyer employee to provide the Services, Supplier shall provide the full name of the individual to Buyer's Contract Administrator or Corporate Procurement Department, prior to any assignment. Buyer, in its sole discretion, reserves the right to decline the assignment of a former Buyer employee to provide the Services.

23.4 Background Check Protocol. Supplier shall provide the last five (5) digits of the social security number (SSN) or equivalent (if an equivalent is provided in lieu of an SSN, Supplier must also provide the date of birth and country of origin) for any Supplier employee, agent, consultant, or subcontractor that performs work under a SOW and is either (a) issued a Buyer "contractor badge" for ingress to and egress from Buyer locations; or (b) given access to any Buyer computer system or environment. If Supplier fails to provide such information, Buyer is under no obligation to issue a contractor badge or give access to such individual. Supplier's performance will not be excused, nor will any obligations of Supplier be limited if Buyer does not issue a contractor badge or provide access in accordance with the terms of this section.

24. Miscellaneous

24.1 Use of Name, Publicity. Supplier shall not, in any manner, advertise, publish, or otherwise make public, the fact that it has furnished, or contracted to furnish, Buyer with the Services without Buyer's prior written consent. Supplier shall not use, display or publish Buyer's logos, brands or trademarks without Buyer's prior written consent.

24.2 Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Michigan.

24.3 Entire Agreement; Amendments. This Agreement constitutes the entire understanding between the parties with respect to the Services. Any Supplier terms and conditions included

with Supplier's invoice or any other document provided by Supplier shall be of no effect. Any terms and conditions set forth in Buyer's purchase order or acknowledgement that are in addition to or in conflict with the terms and conditions are of no effect. No change in the terms of this Agreement will be effective or binding on either party, unless reduced to writing and executed by the respective duly authorized representative of each party.

24.4 Assignment. No party may assign, in whole or in part, its rights or duties under this Agreement to any third party, without the prior written consent of the other party. However, upon prior written notice to Supplier, Buyer may assign or sublicense all or a portion of its rights and responsibilities to an affiliate or to any entity that succeeds to or acquires all or substantially all of the business of the Buyer through merger, consolidation, acquisition of stock or assets, or other business combination. The rights and duties of the parties hereunder shall inure to the benefit of and be binding upon their respective successors and permitted assigns and sublicensees.

24.5 Independent Contractor Status of Parties. Supplier is an independent contractor and not the agent, partner, or employee of Buyer. Supplier and Supplier Personnel are not employees of Buyer and are not entitled to tax withholding, workers' compensation, unemployment compensation, or any employee benefits, statutory or otherwise and shall not cause or allow any third party to reasonably believe that any Supplier Personnel are employees or authorized agents of Buyer, or that Supplier has any grant of authority from Buyer, except as expressly stated in a written agreement between the parties. Supplier shall not have any authority to enter into any contract or agreement to bind Buyer and shall not represent to anyone that Supplier has such authority.

24.6 Headings. Captions and headings are inserted for convenience only and shall not affect the meaning or interpretation.

24.7 Waivers. No delay or omission by either party to exercise any right or remedy under this Agreement shall be construed to be either acquiescence or the waiver of the ability to exercise any right or remedy in the future.

24.8 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions shall nevertheless continue in full force and effect.

24.9 Survivability. Provisions surviving termination or expiration are those which on their face affect rights and obligations after termination or expiration such as provisions concerning indemnification, confidentiality, warranty, and governing law.

24.10 Nondiscrimination. Supplier shall not discriminate against any employee or applicant for employment in its performance of Services, with respect to his or her tenure, terms, conditions, or privileges of employment, or any matter directly or indirectly related to employment because of his or her age, sex, race, color, creed, national origin, or ancestry.

Breach of this covenant may be regarded as a breach of this Agreement and Buyer shall have the right to terminate immediately.

24.11 Accreditation. Supplier shall comply with and adhere to all applicable accreditation standards to which Buyer is subject, as defined in the Services and outlined in the SOW. If Supplier becomes or is accredited under URAC, NCQA or any other nationally recognized accreditation body during the term of this Agreement, Supplier shall maintain such accreditation until the termination or expiration of this Agreement.

24.12 Updates. Supplier acknowledges Buyer may update its Supplier Online Portal from time to time with announcements in which Supplier is obligated to monitor and implement as applicable.

25. Notices

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

25.1.1 To Buyer: Attn: Contract Administrator, Corporate Procurement Department, Blue Cross Blue Shield of Michigan, 600 Lafayette East, Mail Code: 1205, Detroit, MI 48226.

25.1.2 To Supplier: Notices shall be sent to the address listed in the preamble of this Agreement unless otherwise specified herein.

SIGNATURES

Each of the undersigned represents that they are fully authorized to enter into the terms and conditions of, and to execute, this Agreement on behalf of the parties. This Agreement is effective when executed.

Insert Business Entity name(s)	Insert SUPPLIER Name
On behalf of Company	
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT 1

Information Security Requirements

This Information Security Agreement ("ISR"), Contract ID # (XXXXX), is between the Supplier Name ("Supplier"), whose address is Insert Supplier Address, and Blue Cross Blue Shield of Michigan and its affiliates ("Buyer" or "BCBSM"). The Supplier agrees to meet the requirements specified in this Agreement.

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 Buyer data.

2 Information Security Management Program & Policies

2.1 Supplier shall: (a) have an Information Security Management Program ("ISMP") that addresses the overall security program of Supplier's organization; (b) formally implement and document the ISMP; and (c) protect, control, and retain all ISMP records according to federal, state, and internal requirements.

2.2 During the Term of this Agreement and for so long as the Supplier retains BCBSM confidential data after termination, Buyer shall have the right to assess the maturity of the ISMP by reviewing Supplier's information security policies, audit results, analysis of monitored events, preventive measures, and corrective action plans at least annually.

2.3 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.

2.4 Supplier shall develop, publish, and maintain information security policy documentation. The information security policy documentation shall include the purpose and scope of the policy, describe management's and workforce member's roles and responsibilities, and set forth Supplier's approach to establishing information security. The policy documents shall be reviewed no less than annually and updated as needed to ensure policies are current and operationally effective.

2.5 Supplier shall develop, document, and disseminate within Supplier's organization, a risk assessment policy and associated risk assessment controls that consider where applicable, Executive Orders, applicable laws, directives, regulations, policies, standards, and guidelines.
Supplier shall review and update the risk assessment policy at least annually, and risk assessment procedures at least annually or whenever a significant change occurs.

3 Access Management

3.1 Supplier shall develop, publish, and maintain formal access control policies to enforce business and security requirements for access management. Access management policies shall account for Supplier's logical and physical controls. Supplier shall review the policy documents no less than annually and update as needed to ensure policies are current and operationally effective.

3.2 Supplier shall develop, implement, and maintain a documented user registration and de-registration procedure for granting and revoking access. Supplier shall identify user account types, roles, and groups and establish requirements for membership. Supplier shall regularly review all access

privileges of Supplier employees, contractors, and third-party users as required by Supplier's access management policies through a formal documented access review process.

3.3 Supplier shall require users to have unique identifiers for individual access use only. Supplier shall implement authentication and authorization mechanisms for information system and equipment access to verify users' identities.

3.3.1 Supplier shall restrict and control the use of access privileges to information systems and services through a formal documented authorization process. Supplier will only grant users the minimum necessary access privileges for performance of such user's specific job roles and responsibilities.

3.3.2 Supplier shall ensure access rights of all employees, contractors, and third-party users to Buyer's information and information assets shall be removed upon termination of their employment. Supplier shall ensure any changes of employment or other workforce arrangements shall result in a removal of all access rights or modification of access rights that are not required for the new employment or workforce arrangement.

3.3.3 Suppliers shall ensure that passwords are controlled through a formal management process. Supplier shall make users 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.

3.3.4 Supplier shall implement secure authentication methods to control access of remote users to systems containing sensitive information by requiring the use of multifactor authentication mechanisms.

3.4 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. Supplier shall restrict the capability of users to connect to shared networks in line with Supplier's access control policy and requirements of its business applications.

3.4.1 Groups of information services, users and information systems shall be segregated on networks.

3.4.2 Supplier shall implement and maintain firewalls and intrusion detection and prevention 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 Policies

4.1 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.

4.2 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 data.

4.2.1 Supplier shall conduct background verification checks on all candidates for employment, current employees, contractors, and third-party users in accordance with relevant laws and regulations, Buyer's classification of the information to be accessed, and the perceived risks.

4.2.2 A formal disciplinary process shall be established and implemented for employees, contractors, and third-party users who have violated security policies and procedures.

4.3 Supplier shall ensure that all employees, contractors, and third-party users receive appropriate awareness training upon hire and no less than annually thereafter, as well as receive regular updates in Supplier's policies and procedures as relevant to their job function.

5 Risk Management

5.1 Supplier shall create and implement a comprehensive program that manages and mitigates the risk to its information system operations, assets, and Buyer's information.

5.2 Supplier shall perform risk assessments to identify information security risks. Risk assessments are to be performed no less than annually or when major changes occur in the environment, and the results shall be reviewed no less than annually.

6 Risk Management: Artificial Intelligence (AI)

6.1 Supplier shall notify Buyer of any use of AI related to the Services. To the extent Supplier utilizes AI, Supplier shall develop, maintain, and follow an AI risk management program and provide to Buyer upon request. Such program shall identify and quantify risks related to Supplier's development or use of AI and how it intends to mitigate such risks. All risks shall be continually evaluated and assessed by Supplier.

6.2 Supplier shall maintain an inventory of AI data, models, and systems that it uses and/or develops.

6.3 Supplier shall conduct business impact analyses on its AI systems at a minimum annually, considering the criticality of the impact, tangible and intangible impacts, and criteria used to establish the overall impact.

7 Organization of Information Security

6.1 Supplier shall ensure that all Supplier 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 this Agreement.

6.2 Supplier shall review its approach to managing information security, controls, policies, processes, and procedures as needed, but no less than annually.

6.3 Supplier shall adopt and follow an industry recognized cybersecurity framework such as Health Information Trust Alliance ("HITRUST") framework, National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO) 27001, unless Buyer otherwise agrees in writing.

6.3.1 Certifications: Within thirty (30) days of Buyer's written request, Supplier shall, at Supplier's sole cost and expense, begin a SSAE 18 SOC 2 Type II certification (or equivalent, i.e., ISAE 3402) relating to Supplier's business and operations, and provide Buyer with copies of the results as soon as the results are available, but it is no instance longer than six (6) months following Buyer's written request. If Supplier has already performed an annual SSAE 18 SOC 2 Type II certification (or equivalent, i.e., ISAE 3402) within the current year, then Supplier need only provide Buyer with copies of the results of such SSAE 18 SOC 2 Type II certification (or equivalent, i.e., ISAE 3402).

6.4 Supplier shall identify the risks to its information and information assets, including 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.

6.4.1 Supplier shall maintain agreements with its third parties that cover all relevant information security requirements, including as set forth in this Agreements, to the extent that the third parties are accessing, processing, or storing Buyer's data.

6.5 Supplier shall perform risk assessments on its third parties that access, process, and/or store Buyer's data. Supplier agrees to provide evidence of a security assessment of any third parties that have access to Buyer's data.

7 Compliance

7.1 Supplier shall explicitly define, document, and maintain all relevant statutory, regulatory, and contractual requirements for each information system type. Supplier shall similarly define and document the specific controls and individual responsibilities and then communicate them to the user community through a documented security training and awareness program.

7.2 Supplier shall protect all data, documents, information, and records from theft, or loss, or unauthorized or unlawful use, disclosure, modification, alteration, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements.

7.3 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 information. Supplier's compliance with all relevant regulations shall be reviewed at least on an annual basis.

7.4 Supplier shall develop and maintain audit requirements and activities involving checks on operational systems to minimize the risk of disruptions to business processes. Such audit planning and scoping process shall consider risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit.

7.5 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.

8 Asset Management

8.1 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.

8.2 Supplier shall classify information based on its value, relevant legal requirements, sensitivity, and criticality to Supplier.

8.2.1 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.

9 Physical and Environmental Security

9.1 Supplier shall protect secure areas with appropriate physical entry controls to ensure only authorized Supplier Personnel are allowed access. Supplier shall maintain visitor access logs for facilities where information systems reside.

9.2 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 Suppliers Personnel and third-party users.

9.3 Supplier shall design and implement physical security controls for offices, rooms, and facilities to restrict access from the public.

9.4 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. Devices containing

Buyer's data shall be physically destroyed or the information shall be destroyed, deleted, and overwritten using techniques to make the original information non-retrievable.

10 Communications and Operations Management

10.1 Supplier shall formally document and maintain operating procedures for systems associated with information and communication assets and make them available to users on an as-needed basis.

10.2 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.

10.3 Supplier shall establish acceptance criteria for new information systems and any upgrades or new versions of such systems. Supplier shall carry out suitable tests of the systems during development and prior to acceptance to maintain security.

10.4 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.

10.5 Supplier shall separate and control development, test, and operational environments to reduce the risks of unauthorized access or changes to the operational system.

10.6 Supplier shall implement detection, prevention, and recovery controls to protect against malicious and unauthorized code. Supplier shall maintain a formal enterprise IT security policy and user awareness and compliance program. Supplier shall install updates to its anti-virus or anti-spyware software when available. Supplier shall implement and maintain endpoint security controls, firewalls, and data loss prevention solutions to the most current version available. Supplier shall perform periodic reviews on installed software and the data content of systems to identify and, where possible, remove any unauthorized software, malicious code, or viruses.

10.7 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.

10.8 Supplier shall manage and control networks to protect Buyer data from anticipated threats or and to maintain the security and integrity of 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 and 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.

10.9 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 information security 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.

10.9.1 Supplier shall protect media containing Buyer information against unauthorized access, misuse, or corruption during transportation beyond Supplier's physical boundaries.

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

10.11 Supplier shall produce audit logs which record user activities and information security events and Supplier shall maintain such audit logs to assist in future investigations and access control monitoring. Retention for audit logs shall be specified by Supplier and retained accordingly.

10.12 Supplier shall protect logging systems and log information against tampering and unauthorized access.

10.13 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 Information Systems Acquisition, Development, and Maintenance

11.1 Supplier shall implement verification procedures for 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.

11.2 Supplier shall validate application data outputs to ensure that the processing of stored information is correct and appropriate to the circumstances. Supplier shall perform output validation manually or automatically when system development on applications and database is being conducted.

11.3 Supplier shall develop and implement a policy on the use of cryptographic controls and support it with formal procedures. The cryptographic controls policy shall be aligned with the Supplier's information security policy and shall address the use of encryption for protection of Buyer's data transported by removable media devices or across communication lines.

11.4 Supplier shall support the use of cryptographic controls with the practice of key management as set forth in Supplier's cryptographic controls policy. Supplier shall protect all cryptographic keys against modification, loss, and destruction. Supplier shall require protection of secret and private keys against unauthorized disclosure, and all cryptographic keys shall be limited to the fewest number of custodians necessary. Supplier shall physically protect equipment used to generate, store and archive keys, and store encryption keys separately from encrypted data.

11.5 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.

11.6 Supplier shall restrict access to program source code and associated items to prevent the introduction of unauthorized functionality and avoid unintentional changes.

11.7 Supplier shall supervise and monitor outsourced software development. Supplier shall have a contract for the outsourced development in place with the third party which shall address licensing arrangements, certification of the quality and accuracy of the work carried out, warranties to prevent the transfer of malicious code or viruses, 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.

11.8 Supplier shall perform penetration testing and 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. Upon request Supplier shall provide an executive summary report to Buyer of the results of the scans and tests along with a mitigation plan.

12 Information Security Incident Management

12.1 Supplier shall report information security incidents to Buyer pursuant to this Agreement. Supplier shall make all employees, contractors and third-party users aware of their responsibility to report any information security incidents. Supplier shall have documented incident reporting standards and process for employees, contractors and third-party users to report security incidents for further handling.

12.2 Supplier shall implement and maintain an incident response plan containing milestones and criteria 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. Formal information security incident 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 information security incident as discovered, and the timelines of reporting and response.

12.2.1 Supplier shall review the incident response plan no less than annually and include a table-top exercise, documentation, test plan and results.

12.2.2 Supplier shall make revisions to the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

12.3 Supplier shall collect, retain, and present evidence after an information security incident. The evidence that is collected, retained, and presented shall be done in accordance with the laws of the relevant jurisdiction(s).

13 Disaster Recovery Plan and Business Continuity Management

13.1 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 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 shall conduct and review all business continuity planning exercises with all downstream suppliers.

13.2 Supplier shall test and annually review 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 their responsibilities for business continuity and information security.

14 Cloud Security

14.1 This section is applicable only if the Supplier leverages cloud technologies to perform services for or accesses information belonging to the Buyer.

14.2 Supplier shall establish a data protection agreement with its third-party service providers, such as cloud service providers, where Buyer data will be processed or stored.

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

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

14.5 Supplier shall ensure cloud service providers and 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 not less than annually.

14.6 Supplier shall ensure access management controls are implemented in cloud-based environments and applications that will be utilized to process and 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 stored.

14.6.1 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.

14.7 Supplier shall ensure Buyer data that will be stored in cloud-based applications and 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.

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

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

14.10 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.

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

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

14.13 Supplier shall ensure cloud service provider maintains an incident response plan and processes for incident escalation and reporting of information security incidents to Supplier. Supplier shall follow Section 12 (Information Security Incident Management) of this document to review and address the information security 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 2

SUPPLIER SOFTWARE LICENSE

To be Added or Intentionally Omitted

EXHIBIT 3
OFFSHORE LOCATIONS FORM

Table to be completed by Supplier. Buyer approves of the use of the following offshore locations for Supplier Services or Supplier Personnel identified in the SOW (complete each column for each offshore location):

Line #	Name of entity supplying offshore services Subsidiary/Affiliate	Specific offshore location address	General description of services	Will offshore location have	Will offshore location be receiving	Method of access (VDI, VPN, email, excel, secure file transfer, etc.) /	Date location added
1							
2							
3							
4							
5							

If any offshore Services or Supplier Personnel use remote locations other than listed above, Supplier must provide the address of such remote location.