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 the 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 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.

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 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 the 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 the 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 the 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: _____