

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) is entered into by and between (**Kimberly School District**) (the “Covered Entity”) whose principal address is: 141 Center St. W., Kimberly, ID, 83341-1753 and **AssetWorks Risk Management Inc. dba Go Solutions** (the “Business Associate”) whose principal address is: 400 Holiday Drive, Suite 200, Pittsburgh, PA 15220, shall commence on (**July 1st, 2022**) (the “Effective Date”).

RECITALS

WHEREAS, the Covered Entity previously has entered into an underlying agreement with the Business Associate, whereby the Business Associate has agreed to provide certain services to the Covered Entity (the “Service Agreement”);

WHEREAS, to provide such services to the Covered Entity under the Service Agreement, the Business Associate must have access to certain protected health information (“Protected Health Information” or “PHI”), as defined in the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Standards”) set forth by the U.S. Department of Health and Human Services (“HHS”) pursuant to the Health Insurance Portability and Accountability Act of 1996, (“HIPAA”) and amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), part of the American Recovery and Reinvestment Act of 2009 (“ARRA”) and the Genetic Information Nondiscrimination Act of 2008 (“GINA”);

WHEREAS, to comply with the requirements of the Privacy Standards, the Covered Entity must enter into this Agreement with the Business Associate.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter contained, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and intending to be legally bound hereby, the parties hereto agree as follows:

I. Definitions

If terms are used, but not otherwise defined under this Business Associate Agreement, such terms shall then have the same meaning as those terms in the Privacy Rule.

(a) “Covered Electronic Transactions” shall have the meaning given the term “transaction” in 45 CFR §160.103.

(b) “Electronic Protected Health Information” shall have the same meaning as the term “electronic protected health information” in 45 CFR §160.103.

(c) “Individual” shall have the same meaning as the term “individual” in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

(d) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information in 45 CFR Part 160 and Part 164, subparts A and E.

(e) “Protected Health Information (PHI)” shall have the same meaning as the term “protected health information” in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of a Covered Entity.

(f) “Required by Law” shall have the same meaning as the term “required by law” in 45 CFR §164.103.

(g) “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

(h) “Standards for Electronic Transactions Rule” means the final regulations issued by HHS concerning standard transactions and code sets under the Administration Simplification provisions of HIPAA, in 45 CFR Part 160 and Part 162.

(i) “Security Incident” shall have the same meaning as the term “security incident” in 45 CFR §164.304.

(j) “Security Rule” shall mean the Security Standards and Implementation Specifications in 45 CFR Part 160 and Part 164, subpart C.

(k) “Transaction” shall have the meaning given the term “transaction” in 45 CFR §160.103

(l) “Unsecured Protected Health Information” shall have the meaning given the term “unsecured protected health information” in 45 CFR §164.402.

II. Safeguarding Privacy and Security of Protected Health Information

(a) ***Permitted Uses and Disclosures.*** The Business Associate is permitted to use and disclose Protected Health Information that it creates or receives on the Covered Entity’s behalf or receives from the Covered Entity (or another business associate of the Covered Entity) and to request Protected Health Information on the Covered Entity’s behalf (collectively, “Covered Entity’s Protected Health Information”) only:

(i) **Functions and Activities on the Covered Entity’s Behalf.** To perform those services referred in the established services agreement.

(ii) **Business Associate’s Operations.** For the Business Associate’s proper management and administration or to carry out the Business Associate’s legal responsibilities, provided that, with respect to disclosure of the Covered Entity’s Protected Health Information, either:

(A) The disclosure is Required by Law; or

(B) The Business Associate obtains reasonable assurance from any person or entity to which the Business Associate will disclose the Covered Entity's Protected Health Information that the person or entity will:

(1) Hold the Covered Entity's Protected Health Information in confidence and use or further disclose the Covered Entity's Protected Health Information only for the purpose for which the Business Associate disclosed the Covered Entity's Protected Health Information to the person or entity or as Required by Law; and

(2) Promptly notify the Business Associate (who will in turn notify the Covered Entity in accordance with the breach notification provisions) of any instance of which the person or entity becomes aware in which the confidentiality of the Covered Entity's Protected Health Information was breached.

(iii) Minimum Necessary. The Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of the Covered Entity's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that the Business Associate will not be obligated to comply with this minimum-necessary limitation if neither the Business Associate nor the Covered Entity is required to limit its use, disclosure or request to the minimum necessary. The Business Associate and the Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the HITECH Act.

(b) Prohibition on Unauthorized Use or Disclosure. The Business Associate will neither use nor disclose the Covered Entity's Protected Health Information, except as permitted or required by this Agreement or in writing by the Covered Entity or as Required by Law. This Agreement does not authorize the Business Associate to use or disclose the Covered Entity's Protected Health Information in a manner that will violate the Privacy Rule if done by the Covered Entity.

(c) Information Safeguards.

(i) Privacy of the Covered Entity's Protected Health Information. The Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of the Covered Entity's Protected Health Information. The safeguards must reasonably protect the Covered Entity's Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made to a use or disclosure otherwise permitted by this Agreement.

(ii) Security of the Covered Entity's Electronic Protected Health Information. The Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality,

integrity, and availability of Electronic Protected Health Information that the Business Associate creates, receives, maintains, or transmits on the Covered Entity's behalf as required by the Security Rule.

(iii) Policies and Procedures. The Business Associate shall maintain written policies and procedures, conduct a risk analysis, and train its workforce.

(d) Subcontractors and Agents. The Business Associate will require any of its subcontractors and agents, to which the Business Associate is permitted by this Agreement or in writing by the Covered Entity to disclose the Covered Entity's Protected Health Information and/or Electronic Protected Health Information, to provide reasonable assurance that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to the Covered Entity's Protected Health Information and/or Electronic Protected Health Information that are applicable to the Business Associate under this Agreement.

(e) Prohibition on Sale of Records. As of the effective date specified by HHS in final regulations to be issued on this topic, the Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Business Associate obtained from the individual, in accordance with 45 CFR §164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under the HITECH Act.

(f) Penalties for Noncompliance. The Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the privacy rule and security rule, as amended by the HITECH Act.

III. Compliance with the Electronic Transactions Rule

If the Business Associate conducts in whole or part electronic Transactions on behalf of the Covered Entity for which HHS has established standards, the Business Associate will comply, and will require any subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule.

IV. Obligations of the Covered Entity

The Covered Entity shall notify the Business Associate of:

(a) Any limitation(s) in its notice of privacy practices of the Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of Protected Health Information;

(b) Any changes in, or revocation of, permission by the Individual to use or disclose Protected Health Information, to the extent that such changes may affect the Business Associate's use or disclosure of Protected Health Information; and

(c) Any restriction to the use or disclosure of Protected Health Information that the Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of Protected Health Information.

V. Permissible Requests by the Covered Entity

The Covered Entity shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

VI. Individual Rights

(a) **Access.** The Business Associate will, within twenty-five (25) calendar days following the Covered Entity's request, make available to the Covered Entity or, at the Covered Entity's direction, to an individual (or the individual's personal representative) for inspection and obtaining copies of the Covered Entity's Protected Health Information about the individual that is in the Business Associate's custody or control, so that the Covered Entity may meet its access obligations under 45 CFR §164.524. Effective as of the date specified by HHS, if the Protected Health Information is held in an Electronic Health Record, then the individual shall have the right to obtain, from the Business Associate, a copy of such information in an electronic format. The Business Associate shall provide such a copy to the Covered Entity or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously, and specifically made by the individual or the Covered Entity.

(b) **Amendment.** The Business Associate will, upon receipt of written notice from the Covered Entity, promptly amend or permit the Covered Entity access to amend any portion of the Covered Entity's Protected Health Information, so that the Covered Entity may meet its amendment obligations under 45 CFR §164.526.

(c) **Disclosure Accounting.** To allow the Covered Entity to meet its disclosure accounting obligations under 45 CFR §164.528.

(i) **Disclosures Subject to Accounting.** The Business Associate will record the information specified below ("Disclosure Information") for each disclosure of the Covered Entity's Protected Health Information, not excepted from disclosure accounting as specified below, that the Business Associate makes to the Covered Entity or to a third party.

(ii) **Disclosures Not Subject to Accounting.** The Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of the Covered Entity's Protected Health Information if the Covered Entity need not account for such disclosures.

(iii) **Disclosure Information.** With respect to any disclosure by the Business Associate of the Covered Entity's Protected Health Information that is not excepted from disclosure

accounting, the Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:

(A) Disclosure Information Generally. Except for repetitive disclosures of the Covered Entity's Protected Health Information as specified below, the Disclosure Information that the Business Associate must record for each accountable disclosure is (1) the disclosure date, (2) the name and (if known) address of the entity to which the Business Associate made the disclosure, (3) a brief description of the Covered Entity's Protected Health Information disclosed, and (4) a brief statement of the purpose of the disclosure.

(B) Disclosure Information for Repetitive Disclosures. For repetitive disclosures of the Covered Entity's Protected Health Information that the Business Associate makes for a single purpose to the same person or entity (including the Covered Entity), the Disclosure Information that the Business Associate must record is either the Disclosure Information specified above for each accountable disclosure, or (1) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (2) the frequency, periodicity, or number of the repetitive accountable disclosures; and (3) the date of the last repetitive accountable disclosures.

(iv) Availability of Disclosure Information. The Business Associate will maintain the Disclosure Information for at least six (6) years following the date of the accountable disclosure to which the Disclosure Information relates (three (3) years for disclosures related to an Electronic Health Record, starting with the date specified by HHS). The Business Associate will make the Disclosure Information available to the Covered Entity within fifty (50) calendar days following the Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting. Effective as of the date specified by the HHS with respect to disclosures related to an Electronic Health Record, the Business Associate shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual.

(d) Restriction Agreements and Confidential Communications. The Business Associate will comply with any agreement that the Covered Entity makes that either (i) restricts use or disclosure of the Covered Entity's Protected Health Information pursuant to 45 CFR §164.522(a), or (ii) requires confidential communication about the Covered Entity's Protected Health Information pursuant to 45 CFR §164.522(b), provided that the Covered Entity notifies the Business Associate in writing of the restriction or confidential communication obligations that the Business Associate must follow. The Covered Entity will promptly notify the Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct the Business Associate whether any of the Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement. The Business Associate will comply with any restriction request if: (i) except as otherwise Required by Law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and

is not for purposes of carrying out treatment); and (ii) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

VII. Breaches and Security Incidents

(a) Reporting.

(i) Privacy or Security Breach. The Business Associate will report to the Covered Entity any use or disclosure of the Covered Entity's Protected Health Information not permitted by this Agreement along with any Breach of the Covered Entity's Unsecured Protected Health Information. The Business Associate will treat the Breach as being discovered in accordance with 45 CFR §164.410. The Business Associate will make the report to the Covered Entity's Privacy Official not more than fifty (50) calendar days after the Business Associate learns of such non-permitted use or disclosure. If a delay is requested by a law-enforcement official in accordance with 45 CFR §164.412, the Business Associate may delay notifying the Covered Entity for the applicable time period. The Business Associate's report will at least:

(A) Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of the Breach;

(B) Identify the Covered Entity's Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual basis;

(C) Identify who made the non-permitted use or disclosure and who received the non-permitted use or disclosure;

(D) Identify what corrective or investigational action the Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;

(E) Identify what steps the individuals who were subject to a Breach should take to protect themselves; and

(F) Provide such other information, including a written report, as the Covered Entity may reasonably request.

(ii) Security Incidents. The Business Associate will report to the Covered Entity any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of the Covered Entity's Electronic Protected Health Information or (B) interference with the Business Associate's system operations in the Business Associate's information systems, of which the Business Associate becomes aware.

VIII. Term and Termination

(a) **Term.** The term of this Agreement shall commence on the Effective Date and terminate when all Protected Health Information provided by the Covered Entity to the Business Associate, or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

(b) **Right to Terminate for Cause.** The Covered Entity may terminate this Agreement if it determines, in its sole discretion, that the Business Associate has breached any provision of this Agreement, and upon written notice to the Business Associate of the breach, the Business Associate fails to cure the breach within thirty (30) calendar days after receipt of the notice. Any such termination will be effective immediately or at such other date specified in the Covered Entity's notice of termination.

(i) Return or Destruction of Covered Entity's Protected Health Information as Feasible.

Upon termination or other conclusion of this Agreement, the Business Associate will, if feasible, return to the Covered Entity or destroy all of the Covered Entity's Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of the Covered Entity's Protected Health Information. This provision shall apply to the Covered Entity's Protected Health Information that is in the possession of subcontractors or agents of the Business Associate. Further, the Business Associate shall require any such subcontractor or agent to certify to the Business Associate that it returned to the Business Associate (so that the Business Associate may return it to the Covered Entity) or destroyed all such information which could be returned or destroyed. The Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of this Agreement.

(ii) Procedure When Return or Destruction Is Not Feasible. The Business Associate will identify any of the Covered Entity's Protected Health Information, including any that the Business Associate has disclosed to subcontractors or agents as permitted under this Agreement, that cannot feasibly be returned to the Covered Entity or destroyed and explain why return or destruction is infeasible. The Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. The Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of this Agreement.

(iii) Continuing Privacy and Security Obligation. The Business Associate's obligation to protect the privacy and safeguard the security of the Covered Entity's Protected Health

Information as specified in this Agreement will be continuous and survive termination or other conclusion of this Agreement.

IX. Miscellaneous Provisions

(a) **Definitions.** All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance.

(b) **Inspection of Internal Practices, Books, and Records.** Upon reasonable prior written notice, the Business Associate will make its internal practices, books, and records relating to its use and disclosure of the Covered Entity's Protected Health Information available to the Covered Entity and to HHS during regular business hours to determine compliance with the Privacy Rule.

(c) **Amendment to Agreement.** Upon the compliance date of any final regulation or amendment to final regulation promulgated by HHS that affects the Business Associate or the Covered Entity's obligations under this Agreement, this Agreement will automatically amend such that the obligations imposed on the Business Associate or the Covered Entity remain in compliance with the final regulation or amendment to the final regulation.

(d) **No Third-Party Beneficiaries.** Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.

(e) **Regulatory References.** A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

(f) **Survival.** All provisions of this Agreement, which by their nature should survive termination of this Agreement, will so survive.

(g) **Interpretation.** Any ambiguity in this Agreement shall be resolved to permit the Covered Entity to comply with the Privacy Rule.

(h) **Notices.** All notices hereunder shall be in writing and delivered by hand, by certified mail, return receipt requested, by overnight delivery, or facsimile or electronic mail transmission with receipt acknowledged. Notices shall be directed to the parties at their respective addresses set forth below their signature, as appropriate, or at such other addresses as the parties may from time to time designate in writing.

(i) **Entire Agreement; Modification.** This Agreement represents the entire agreement between the Business Associate and the Covered Entity relating to the subject matter hereof. No provision of this Agreement may be modified, except in writing, signed by the parties.

(j) **Binding Effect.** This Agreement shall be binding upon the parties hereto and their successors and assigns.

IN WITNESS WHEREOF, the parties, through their authorized representatives, have executed this Agreement as of the Effective Date.

“Business Associate” – AssetWorks Risk Management Inc. dba Go Solutions

Signature: _____

Print Name: _____

Title: _____

Date: _____

“Covered Entity” – Kimberly School District

Signature: _____

Print Name: _____

Title: _____

Date: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____

SOFTWARE AS A SERVICE AGREEMENT

This Software as a Service Agreement (“Agreement”) is effective July 1, 2022, and entered into between AssetWorks Risk Management Inc. dba Go Solutions (“AssetWorks”), with offices at 400 Holiday Drive, Suite 200, Pittsburgh, PA 15220 and Kimberly School District (“Client”), with offices at 141 Center St. W., Kimberly, ID, 83341- 1753. In consideration of the mutual covenants contained herein, the parties agree as follows:

1. Software as a Service, Maintenance, and Services. Subject to the terms and conditions of this Agreement and the payment of fees hereunder, AssetWorks will provide Client with the following:

1.1 Software as a Service. AssetWorks will provide Client with access, through a website or designated IP address, to its proprietary software identified on Schedule A (“Software”) which is maintained by AssetWorks in a hosted environment at a third-party data center (“SaaS”).

1.2 Maintenance.

1.2.1 AssetWorks will provide: (i) support during normal business hours (Monday through Friday, excluding legal holidays) relating to the operation of the Software and use of the SaaS and (ii) Updates to the Software as they are developed and made generally available (“Maintenance”). Requests for support may be submitted to AssetWorks by Client via methods provided by AssetWorks). “Update” means the latest updates, modifications, and enhancements to the Software, including corrections of errors, which relate to the operating performance of the Software.

1.2.2 Maintenance does not include: (a) custom programming services; (b) on-site support, including installation of hardware or software; (c) support of any software other than the Software accessed as part of the SaaS; (d) training; (e) expenses for third party products including, but not limited to, hardware and related supplies; (f) support of Client’s computer system, software, or hardware (e.g., computer equipment, servers, printers etc.) or third party software or hardware, including problems which arise therefrom. For clarity, AssetWorks is not responsible for errors or defects of Client or third-party software or hardware.

1.3 Services. AssetWorks will provide Client with services including, but not limited to, data conversion, system configuration, interface provisioning, professional development, training, consultation, custom reporting, custom changes, programming, and other related services selected by Client and identified in Schedule A or a separate signed quote or statement of work referencing this Agreement (“Services”). Administrative, reimbursement, and audit Services provided in support of the SaaS will be performed in accordance with Section 11.2. The Services do not include Maintenance.

2. Rights and Permitted Use.

2.1 Subscription. Subject to the terms and conditions of this Agreement, AssetWorks grants to Client a non-exclusive and non-transferable subscription for Authorized Users to access and use the SaaS and Documentation for Client’s internal business operations. “Authorized Users” mean Client’s employees or independent contractors working within their job responsibilities or engagement by Client or other end user for which AssetWorks has granted Client the right to use the SaaS. “Documentation” means documentation in the form of instructions and manuals provided by AssetWorks, including electronically via a link within the SaaS, that describes the function and use of the SaaS.

2.2 Restrictions. Client will not (i) directly or indirectly decompile, disassemble, reverse engineer, or otherwise attempt to discover the source code or underlying structure, ideas, know-how or algorithms relevant to the SaaS, Software, Documentation, or any data related to the SaaS; (ii) copy, modify, enhance, translate, change the data structures for or create derivative works from, the SaaS; (iii) rent, lease, sell, or otherwise provide access to the SaaS to any third party or to anyone other than Client’s Authorized Users; (iv) interfere with or disrupt the integrity or

performance of the SaaS or third party data contained therein; (v) attempt to gain unauthorized access to the SaaS or its related systems or networks; or (vi) remove any proprietary notices or labels.

2.3 Ownership. AssetWorks owns all intellectual property rights in and to: (i) the Software, including all Updates; (ii) the SaaS; (iii) any Documentation or data related to the Software or the SaaS; and (iv) any software, applications, inventions or other technology provided or developed in connection with the Software or the SaaS. For clarity, Client obtains no interest in the Software, SaaS, or Documentation except as expressly provided in this Agreement.

2.4 Client Data. Client shall retain all right, title, and interest in and to the data which is Client created or owned and provided to AssetWorks or to which AssetWorks has access in connection with the Services or use of the SaaS, including Client information, data, records, and reports ("Client Data"). Client shall, in a timely manner, provide AssetWorks with all reasonably requested Client Data determined by AssetWorks as necessary for performing the Services. Client grants to AssetWorks a royalty-free, non-exclusive, non-transferable license for the Term of this Agreement to use Client Data to the extent necessary to provide the SaaS, Services, and Maintenance. Notwithstanding anything to the contrary, AssetWorks shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the SaaS and related systems and technologies (including, without limitation, information concerning Client Data and data derived therefrom), and AssetWorks will be free (during and after the Term hereof) to: (i) use such information and data to improve and enhance the SaaS and for other development, diagnostic and corrective purposes in connection with the SaaS and other AssetWorks offerings, and (ii) disclose such data solely in aggregate or other de-identified form in connection with its business.

3. Fees and Payment.

3.1 Fees. Client shall pay the fees set forth in Schedule A. AssetWorks may increase the fees on an annual basis.

3.2 Payment. Client agrees to pay all fees within thirty (30) days of the invoice date. With regard to any invoiced amount that is not paid when due, AssetWorks reserves the right to charge, and Client agrees to pay, a late payment fee on the unpaid balance from the due date until paid equal to the lesser of one and one half percent (1.5%) per month, or the maximum amount allowable by law. All fees are non-refundable, except as otherwise explicitly stated in this Agreement.

4. Term and Termination.

4.1 Term. This Agreement shall commence on the Effective Date and continue for a term of one (1) year ("Initial Term"). Thereafter, this Agreement shall automatically renew for additional terms of one (1) year (each, a "Renewal Term") unless either party provides written notice to the other party at least thirty (30) days prior to the expiration of the then current Term. The Initial Term and any Renewal Term are collectively referred to as the "Term" of this Agreement.

4.2 Termination. Either party may terminate this Agreement immediately upon written notice if the other party breaches any material provision of this Agreement and does not cure the breach within thirty (30) days after receiving written notice thereof.

4.3 Effect of Termination. Upon termination of this Agreement, Client's subscription to the SaaS will end and Client shall immediately cease using the SaaS and, if requested, certify to AssetWorks within thirty (30) days after termination that Client has deleted or destroyed any copies of Documentation in its possession. If the Agreement is terminated, upon Client's request provided at least thirty (30) days prior to the date of termination, AssetWorks will provide a standard media download of the Client Data for an additional fee charged at AssetWorks' standard rates. Custom downloads or handling of Client Data are subject to an additional fee. Termination of this Agreement shall not release Client from the obligation to pay fees due hereunder for the SaaS, Maintenance, and Services provided prior to

the date of termination. AssetWorks may maintain records related to this Agreement after termination as required in accordance with applicable laws, subject to Section 5.

4.4 Suspension or Termination of SaaS. AssetWorks may suspend or terminate Client's access to the SaaS if Client fails to pay any fees when due which remain unpaid for thirty (30) days after receipt of written notice. AssetWorks reserves the right to temporarily suspend the SaaS based on its good faith belief that it is necessary to protect the integrity of the SaaS. If the Agreement is terminated pursuant to this Section 4, AssetWorks may terminate Client's access to the SaaS as of the termination date.

5. Confidentiality.

5.1 Confidential Information. Each party (the "Disclosing Party") may from time to time during the Term of this Agreement disclose to the other party (the "Receiving Party") certain information relating to trade secrets, data, designs, drawings, documentation, software (regardless of form or media), prototypes, processes, methods, concepts, research, development, facilities, employees, vendors, clients, marketing, financials, business activities, and other confidential or proprietary information (collectively "Confidential Information"). To the extent practicable, the Disclosing Party shall mark and/or identify Confidential Information as confidential or proprietary at the time of disclosure; provided however, this Agreement shall also apply to information which, based on its nature, is reasonably expected to be deemed confidential. In addition, the terms of this Agreement shall be deemed Confidential Information. Furthermore, whether or not so marked or identified, the Software, Documentation and any related data, and any quantitative analysis of the Software or performance of the Software are deemed the Confidential Information of AssetWorks, and the Client Data is deemed the Confidential Information of Client.

5.2 Exceptions. Confidential Information shall not include information that: (a) becomes generally available to the public through no fault of the Receiving Party; (b) is lawfully provided to the Receiving Party by a third party not under an obligation of confidentiality; (c) was lawfully possessed by the Receiving Party prior to receiving the Confidential Information from the Disclosing Party, as evidenced by the Receiving Party's records; or (d) the Receiving Party can demonstrate was independently developed by Receiving Party without use of the Disclosing Party's Confidential Information. The Receiving Party may disclose Confidential Information pursuant to applicable law, regulation, court order, or other legal process; provided, (i) if allowed by law, the Receiving Party has given the Disclosing Party prompt written notice of such required disclosure so that the Disclosing Party may seek a protective order or other appropriate remedy and (ii) the Receiving Party discloses only that portion of the requested Confidential Information that, in the opinion of its legal counsel, it is required to disclose.

5.3 Non-Disclosure and Non-Use. The Receiving Party agrees that it shall not use Confidential Information, or disclose any Confidential Information to any third party, except as expressly permitted under this Agreement. The Receiving Party shall not provide access to the Confidential Information to anyone other than those of its employees, contractors, and financial and legal advisors who have a need to know, who have confidentiality obligations no less restrictive than those set forth herein, and who have been informed of the confidential nature of such information. The Receiving Party shall protect the Confidential Information from unauthorized use, access, or disclosure in the same manner as it protects its own confidential or proprietary information of a similar nature, and in any event with at least a reasonable degree of care.

6. Service Availability.

6.1 The SaaS includes a target scheduled availability of ninety-nine percent (99%) (exclusive of scheduled maintenance or any downtime attributable to Client or third parties, or for which AssetWorks is not responsible including, but not limited to interruptions and delays inherent in internet communications).

6.2 AssetWorks will use commercially reasonable efforts to ensure that the web pages generated with the SaaS will be served (i.e., delivered from AssetWorks' internal network or that of its internet service provider) promptly regardless of the level of traffic to AssetWorks' servers, subject to outages, communication and data flow failures, interruptions and delays inherent in internet communications. Client acknowledges that problems with the internet, equipment, software and network failures, impairments or congestion, or the configuration of Client's computer systems, may prevent, interrupt or delay Client's access to the SaaS or data stored within the SaaS. AssetWorks is not liable for any delays, interruptions, suspensions, or unavailability of the SaaS or the data stored within the SaaS beyond AssetWorks' control, attributable to problems with the internet or the configuration of Client's computer systems.

7. Data.

7.1 Client is solely responsible for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Client Data. Client will not submit or store infringing, obscene, threatening, libelous or otherwise unlawful or tortious material, including material that violates third party privacy or intellectual property rights, includes malicious code, or that will interfere with the integrity of the SaaS.

7.2 Each party agrees that, in the performance of its respective obligations under this Agreement, it shall comply with the provisions of applicable data protection laws to the extent it applies to each of them. Accordingly, AssetWorks agrees that it shall: only process Client's personal data in order to provide the SaaS or in accordance with any lawful instructions reasonably given by Client from time to time; (ii) implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and accidental destruction or loss; and (iii) as soon as reasonably practicable, refer to Client any requests, notices, or other communication from data subjects, data protection or other law enforcement authority, for Client to resolve.

7.3 AssetWorks shall notify Client as soon as reasonably possible upon discovery of any data security incident impacting Client Data. AssetWorks shall not be responsible for any loss or damage to Client Data to the extent that such loss or damage was caused by Client or a third party.

8. Representations and Warranties.

8.1 General Warranty. Each party represents and warrants: (i) it has the full power and authority to enter into this Agreement; (ii) its execution and performance of this Agreement have been duly authorized by all necessary corporate action on behalf of such party; and (iii) the person signing this Agreement on behalf of such party has the full authority to do so.

8.2 Limited Warranty. AssetWorks warrants the SaaS will conform in all material respects to the Documentation and the Services will be provided in compliance with the terms of this Agreement. The warranties set forth in this Section 8.2 will not apply if: (i) the SaaS is not used in accordance with AssetWorks' instructions, the Documentation, or the terms of this Agreement; (ii) the SaaS is used in combination with other software, data, or products that are incompatible with the SaaS; (iii) the SaaS has been altered, modified, or converted by anyone other than AssetWorks; or (iv) non-conformance or non-compliance is caused by (a) a defect or malfunction in the operating system, database server, web server, network, or other hardware or software in Client's computer system used to access the SaaS, (b) Client's failure to perform its responsibilities hereunder, or (c) Client's negligence or willful misconduct. Client's exclusive remedy, and AssetWorks' sole liability, for breach of this warranty shall be for AssetWorks to use commercially reasonable efforts to correct errors affecting conformance or compliance, provided that Client has given written notice of non-conformance or non-compliance to AssetWorks within ninety (90) days of discovery of the error. AssetWorks shall, to the extent reasonably possible and permissible, pass-through or assign to Client all available warranties it receives from a third-party provider for third party products or services provided by AssetWorks to Client under this Agreement.

8.3 Disclaimer of Warranties. EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, THE SOFTWARE, SAAS, MAINTENANCE, SERVICES, DOCUMENTATION, AND THIRD PARTY PRODUCTS AND SERVICES, IF ANY AND AS APPLICABLE, ARE PROVIDED "AS IS", AND ASSETWORKS DISCLAIMS ALL OTHER WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR THAT THE SOFTWARE, SAAS, MAINTENANCE, SERVICES, DOCUMENTATION, AND THIRD PARTY PRODUCTS OR SERVICES, IF ANY AND AS APPLICABLE, WILL MEET ALL OF CLIENT'S REQUIREMENTS.

8.4 Client Responsibilities. Client represents that it is fully responsible for: (a) the content of any Client Data; (b) assigning a primary Client representative to coordinate with AssetWorks regarding the SaaS, Services, and Maintenance; (c) selection and implementation of controls, including settings and policies, regarding access rights and use of the Software by Client and its Authorized Users; (d) Client's computer system, software, and hardware (e.g., computer equipment, servers, printers etc.); (e) reasonably analyzing suspected problems to determine their specific nature and possible causes before contacting AssetWorks for assistance and then subsequently informing AssetWorks of any problems encountered in a timely manner; (f) enlisting clinicians with appropriate background and credentials to conduct screening examinations, as applicable, and review such clinician credentials to determine whether they are meet State specified minimum criteria; (g) making good faith efforts to successfully pursue and defend reimbursement claims filed with the State, local government, or any agency or department thereof relating to the Services, including without limitation, assistance in grant appeals and all other legal proceedings. Client acknowledges that the SaaS is intended to perform with the system requirements specified in the Documentation or instructions provided by AssetWorks to Client, as those may be updated from time to time. AssetWorks assumes no responsibility for: (i) failure of the SaaS based upon Client's failure to comply with such system requirements; (ii) the correctness or performance of, or any resulting incompatibilities with, current or future releases of the Software if Client has made changes to its system hardware/software configuration without prior notification and written approval by AssetWorks; or (iii) operation or performance of any Client or third-party application.

9. Indemnification.

9.1 AssetWorks will defend and indemnify Client against any claim, action, suit, or proceeding brought by a third party ("Claim") to the extent Client's use of the SaaS within the scope of this Agreement directly infringes a United States patent or copyright issued to or held by a third party, or misappropriates a trade secret of such third party; provided, that Client notifies AssetWorks promptly in writing of such Claim and provides AssetWorks with the sole control, authority, information and assistance necessary to defend or settle such Claim.

9.2 In the event of an infringement Claim, or AssetWorks believes that such a Claim is likely, then AssetWorks shall, at its expense: (i) procure the right for Client to continue using the SaaS; (ii) replace or modify the SaaS so that it becomes non-infringing, without materially decreasing the functionality of the SaaS; or (iii) if neither (i) or (ii) is commercially practical, then, at AssetWorks' sole option, terminate this Agreement and refund a portion of the SaaS fee paid by Client for the period in which the SaaS was affected by such infringement.

9.3 AssetWorks will not be liable for any infringement Claim based upon any (i) modification of the SaaS made by anyone other than AssetWorks; (ii) use of the SaaS in combination with any software or other technology not supplied by AssetWorks or in which the SaaS was not intended to be used as specified in the Documentation, to the extent such Claim would not have arisen but for such combination (regardless of whether or not AssetWorks has advised Client that such use would likely result in a Claim of infringement by a third party); or (iii) use of the SaaS contrary to the terms of this Agreement or the Documentation.

9.4 THE FOREGOING STATES ASSETWORKS' SOLE AND EXCLUSIVE LIABILITY AND THE SOLE AND EXCLUSIVE REMEDY OF CLIENT WITH RESPECT TO ANY CLAIM OF INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OR PROPRIETARY RIGHTS OF ANY THIRD PARTY.

9.5 Client shall defend and indemnify AssetWorks from and against any and all Claims, liabilities, damages, costs, and expenses, including reasonable legal fees, arising from or related to the exclusions set forth in Section 9.3 or any violation of Sections 2.2 or 7.1.

10. Limitation of Liability.

10.1 Neither party shall be liable for any indirect, incidental, consequential, exemplary, special, or punitive damages including, without limitation, any damages resulting from loss of use, loss of business, loss of revenue, loss of profits, or loss of data, even if a party has been advised of the possibility of such damages.

10.2 AssetWorks' entire liability under this Agreement or in any way related to the SaaS, Maintenance, or Services will be limited to direct damages in an amount equal to the fees paid by Client to AssetWorks pursuant to this Agreement during the twelve (12) month period immediately preceding the Claim.

11. General.

11.1 **Governing Law.** This Agreement shall be governed by and interpreted in accordance with the laws of the State in which Client resides without regard to conflicts of law principles.

11.2 **Compliance with Laws.** Each party will perform its responsibilities hereunder in compliance with all federal, state, and local laws, rules, and regulations applicable to such party.

11.3 **Severability.** If any provision of this Agreement is held by a court of competent jurisdiction to be unenforceable for any reason, such provision will be changed and interpreted to accomplish the objectives of such provision to the greatest extent possible under applicable law and the remaining provisions hereof shall be unaffected and remain in full force and effect.

11.4 **Modification and Waiver.** Any modification, amendment, supplement, waiver, or other change to this Agreement must be in writing and signed by duly authorized representatives of each party. Any waiver or failure to enforce any provision of this Agreement on any occasion shall not be deemed a waiver of any other provision or of such provision on any other occasion.

11.5 **Assignment.** Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other party's prior written consent, which shall not be unreasonably withheld; provided, however, either party may assign this Agreement in its entirety, without the other party's consent, in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. This Agreement shall be binding upon and inure to the benefit of the successors in interest and permitted assigns of the respective party.

11.6 **Remedies.** The parties agree that monetary damages are an inadequate remedy for breach of Sections 2 and 5, and further recognize that any such breach would cause irreparable injury for which there would be no adequate remedy at law; therefore, the parties agree that the non-breaching party may seek equitable remedies, including, without limitation, injunctive relief and specific performance (without obligation to post a bond) from a court of competent jurisdiction, in addition to other remedies available at law or in equity.

11.7 **Survival.** All provisions of this Agreement, which by their nature should survive termination of this Agreement, will so survive.

11.8 **Force Majeure.** Neither party shall be in breach of this Agreement, nor liable for delay in performing or failure to perform any of its obligations under this Agreement, if such delay or failure result from unforeseeable events, circumstances, or causes beyond its reasonable control, including, but not limited to: natural hazards or acts of nature

(such as floods, fires, earthquakes, hurricanes, or explosions); governmental acts or omissions (such as expropriation, condemnation, and changes in laws or regulations); acts of war (whether declared or undeclared); acts of the public enemy and terrorism; strikes and labor disputes; civil commotion; epidemics, pandemics and quarantine; infrastructure failures (such as transportation, energy, or breakdown of communication facilities); and delays of either party's suppliers for like causes; provided that the party affected by such failure or delay gives the other party prompt written notice of the cause and uses commercially reasonable efforts to correct such failure or delay within a reasonable period of time.

11.9 Headings. The headings and subheadings contained herein are inserted for convenience of reference only and shall in no way be construed to be interpretations of terms.

11.10 Notices. All notices under this Agreement shall be in writing and shall be deemed given upon personal delivery, delivery by prepaid overnight courier, facsimile or electronic mail transmission with receipt acknowledged, or three (3) business days after deposit in the mail via first class mail postage prepaid to the intended recipient at its address listed above or other such address as the parties may indicate in writing.

11.11 Entire Agreement. This Agreement, including schedules or other attachments hereto and any amendments or written documentation executed by the parties, are the final, complete, and exclusive agreement between the parties relating to the subject matter hereof, and supersede all prior or contemporaneous proposals, understandings, representations, warranties, promises, and other communications, whether oral or written, relating to such subject matter.

11.12 Counterparts. This Agreement, and any amendment or waiver of the terms hereof, may be signed in counterparts, each of which will constitute an original and all of which together will constitute one and the same instrument. Any signature may be delivered by facsimile or electronic format, which will have the effect of an original signature.

The parties, through their authorized representatives, have executed this Agreement as of the Effective Date.

Kimberly School District

AssetWorks Risk Management Inc.
dba Go Solutions

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

SCHEDULE A

This Schedule A sets forth details regarding the SaaS subscription and services (if applicable) and the corresponding fees.

QUANTITY	ITEM DESCRIPTION	AMOUNT
1	SET-UP AND IMPLEMENTATION (including initial database setup, integration implementation, on-going capacity planning, backup, archival and retrieval subsystems, security monitoring)	Included
1	MEDICAID ELIGIBILITY VERIFICATION (including on-going 270 submission, 271 retrieval and processing, and manual verification if necessary)	Included
1	ENCOUNTER VERIFICATION (including review of proper CPT and ICD10 coding, review of applicable CPT code limits, and IEP prescribed service comparison)	Included
1	CLAIM SUBMITTAL (generation of 837 transaction set and interface with the State for submission, TA1 and 997 transaction set processing to ensure valid transfer)	Included
1	REMITTANCE ADVICE BALANCING (loading and processing of the 835 transaction set, including payment posting and balancing of submitted versus received)	Included
1	DENIAL REVIEW AND RESUBMISSION (claim and service line level review of denied claims, review of student eligibility, provider licensing, that could result in resubmissions)	Included
1	MANAGEMENT REPORTS TRAINING	Included
1	ON-GOING SYSTEM MODIFICATIONS (required State and/or Federal system modifications)	Included
1	ON-GOING USER AND ADMINISTRATOR SUPPORT	Included
1	Physician Referrals (no claims will be submitted without ensuring that a timely referral has been obtained for the services identified in the student's IEP).	Included
1	Guardian Digital Signatures	Fee Available Upon Request
1	Additional Modules: Section 504 English Learner Data Management RTI/MTSS	Fee Available Upon Request
Fee:		Fee: 6% administrative fee for all Medicaid reimbursements.