AGREEMENT
Between
THE CITY OF COLUMBIA, MISSOURI
And
IMAGENET CONSULTING, LLC

THIS AGREEMENT (hereinafter "Agreement") between the City of Columbia, Missouri, a municipal corporation (hereinafter "CITY") and ImageNet Consulting, LLC, a limited liability company organized in the State of Oklahoma, (hereinafter "CONSULTANT") is entered into on the date of the last signatory noted below (the "Effective Date"). CITY and CONSULTANT are each individually referred to herein as a "Party" and collectively as the "Parties."

WITNESSETH:

WHEREAS, City desires to engage the Consultant to provide Laserfiche Subscription based user Licenses and to render certain related professional services as outlined in the Scope of Work in Exhibit A; and

WHEREAS, Consultant represents and warrants that Consultant is equipped, competent, and able to provide the subscription based licenses and all of the professional services necessary or appropriate in accordance with this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants set out in this Agreement and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged), the Parties agree as follows.

1. Services and Performance Standards.

a. Scope of Services. The scope of services involves the provision of subscription based Laserfiche licenses and related professional and technical consulting services for **Implementation Services** (hereinafter "Project"). The Project is more fully described in CONSULTANT's **Scope of Services**, which is attached as **Exhibit A**.

b. Prior to beginning any work on Project, CONSULTANT shall resolve with CITY any perceived ambiguity in Project. CITY shall issue a written notice to proceed. CONSULTANT shall not prepare a written report unless the CITY directs CONSULTANT to do so.

c. CONSULTANT shall exercise reasonable skill, care and diligence in performance of its services and will carry out its responsibilities in accordance with the generally accepted standards of good professional practices in effect at time of performance. If CONSULTANT fails to meet the foregoing standards, CONSULTANT shall perform at its own cost, and without reimbursement from

CITY, the professional services necessary to correct errors and omissions which are caused by CONSULTANT's failure to comply with the above standard.

d. Schedule. On or after the Effective Date, the CITY shall issue the notice to proceed. Within thirty days of the notice to proceed, the parties shall agree in writing to a schedule of work. CONSULTANT shall proceed in accordance with the timeline contained in the Schedule of Work, set forth in Exhibit B. The start date on the Schedule of Work shall be the "Commencement Date."

2. Addition or Deletions.
a. CITY may add to CONSULTANT's services or delete therefrom, provided that the total cost of such work does not exceed the total cost allowance as specified herein. CONSULTANT shall undertake such changed activities only upon the written direction of CITY. All such directives and changes shall be in written form and prepared and approved by the Parties. There shall be no change in the Schedule of Work unless specifically identified and agreed to by CONSULTANT and CITY at the time such services are added or deleted.
b. CITY may increase or decrease the number of license subscriptions. Annually, CONSULTANT shall invoice CITY for the number of license subscriptions based upon the pricing set forth in Exhibit C.

3. Exchange of Data. All information, data, and reports in CITY's possession and necessary for the carrying out of the work, shall be furnished to CONSULTANT without charge, and the Parties shall cooperate with each other in every way possible in carrying out the Scope of Services.

4. Personnel. CONSULTANT represents that CONSULTANT will secure at CONSULTANT's own expense, all personnel required to perform the services called for under this Agreement by CONSULTANT. Such personnel shall not be employees of or have any contractual relationship with CITY, except as employees of CONSULTANT. All of the services required hereunder will be performed by CONSULTANT or under CONSULTANT's direct supervision. All CONSULTANT's personnel engaged in the work shall be fully qualified and shall be authorized under state and local law to perform such services. None of the work or services covered by this Agreement shall be subcontracted without the prior written approval of CITY.

5. Term; Renewal; Termination.
a. Implementation Services. Implementation Services shall commence on the Commencement Date and shall conclude upon completion of the Implementation and acceptance by the CITY (hereinafter "Date of Completion of Implementation Services").
b. Annual Laserfiche Subscription and annual Maintenance (hereinafter collectively, "Subscription"). The annual Subscription Term shall commence on the Date of Initiation of Implementation Services and shall continue until the date that is one year following the Date of Initiation of Implementation Services.

Thereafter, the Subscription term shall automatically renew for successive terms of one year, unless the Agreement is terminated pursuant to the provisions of this Agreement.

6. Costs not to Exceed.

a. Implementation and Integration Services. CITY agrees to pay CONSULTANT at the rates set forth in the Pricing Sheet contained in Exhibit C attached hereto in a total amount not to exceed the sum of **one hundred eighty-six thousand six hundred and forty dollars ($186,640.00)**.

b. Subscriptions. CITY agrees to pay CONSULTANT at the rates set forth in the Pricing Sheet contained in Exhibit C attached hereto in a total amount not to exceed the sum of sixty-six thousand two hundred and twenty-five dollars ($66,225.00) per year. The subscription price shall remain firm for a period of five years. After the 5 year price lock period, the subscription price can increase no more than 5% year over year.

c. Years 2 through 5 Maintenance of the Tyler Energov Integration. CITY may elect to pay CONSULTANT for maintenance of the Tyler Energov Integration at a rate of two thousand four hundred dollars ($2,400.00) per year for years two through five. Thereafter, the maintenance fee can increase no more than five percent year over year.

7. Payment.

a. CONSULTANT may issue an invoice on a monthly basis for work performed and expenses since the preceding invoice or, if there was no preceding invoice, since the issuance of a notice to proceed.

b. Conditioned upon acceptable performance. Provided CONSULTANT performs the services in the manner set forth in Paragraph 1 hereof, CITY agrees to pay CONSULTANT in accordance with the terms outlined herein, which shall constitute complete compensation for all services to be rendered and licenses provided under this Agreement; provided, that where payments are to be made periodically to CONSULTANT for services rendered under this Agreement, CITY expressly reserves the right to disapprove in whole or in part a request for payment where the services rendered during the period for which payment is claimed are not performed in a timely and satisfactory manner.

c. CITY shall have ten (10) days from the date of receipt of the invoice to register CITY's disapproval of the work billed on that invoice. Following CONSULTANT's receipt of said disapproval, CONSULTANT shall have ten (10) days to cure the issues presented. If cure cannot be obtained within ten (10) days, CONSULTANT shall notify CITY of the proposed amount of time for cure, and reach an agreement as to an acceptable alternative deadline.

d. Upon receipt of the invoice and progress report, CITY will, as soon as practical, pay CONSULTANT for the services rendered. CITY shall pay CONSULTANT within thirty (30) days of receipt of an invoice.

8. Termination by Default.

a. Events of Default. A Party shall be considered in Default of this Agreement upon: (1) The failure to perform or observe a material term or condition of this Agreement, including but not limited to any material Default of a representation, warranty or covenant made in this Agreement; (2) The Party (i) becoming insolvent; (ii) filing a voluntary petition in bankruptcy under any provision of any federal or state bankruptcy law or consenting to the filing of any bankruptcy or reorganization petition against it under any similar law; (iii) making a general assignment for the benefit of its creditors; or (iv) consenting to the appointment of a receiver, trustee or liquidator; (3) The purported assignment of this Agreement in a manner inconsistent with the terms of this Agreement; (4) The failure of the Party to provide information or data to the other Party as required under this Agreement, provided that the Party entitled to the information or data under this Agreement requires such information or data to satisfy its obligations under this Agreement.

b. Termination upon Default. Upon the occurrence of an event of Default, the non-Defaulting Party shall be entitled to terminate the agreement with thirty (30) days written notice.

9. Additional Termination Clauses.

a. By Mutual Agreement. This Agreement may be terminated at any time during its Term upon mutual agreement by both Parties.

b. By Convenience. With thirty (30) days written notice, the City may terminate the Agreement for convenience.

c. By Force Majeure. The agreement may be terminated due to force majeure. The performance of each Party under the Agreement may be subject to interruptions or reductions due to an event of Force Majeure. The term "Force Majeure" shall mean an event or circumstance beyond the control of the Party claiming Force Majeure, which, by exercise of due diligence and foresight, could not reasonably have been avoided, including, but not limited to, flood, earthquake, storm, fire, lightning, epidemic, war, riot, civil disturbance, sabotage, strike, and act of God or any other cause beyond the control of the Party claiming Force Majeure. However, the obligation to use due diligence shall not be interpreted to require resolution of labor disputes by acceding to demands of the opposition when such course is inadvisable in the discretion of the Party having such difficulty. A Party shall not be liable to the other Party in the event it is prevented from performing its obligations hereunder in whole or in part due to an event of Force Majeure.

d. Effect of Termination. Within ten (10) days after receiving notice of termination, the contractor shall provide City with a copy of all City data and content in a format acceptable to the City at no cost to the City.

10. Red Flag Policy Compliance. CONSULTANT agrees to comply with the City's Red Flag Policy and any Amendment thereto, a copy of which is attached to this Agreement as Exhibit D. CONSULTANT shall provide City with a copy of its existing red flag policies and procedures, shall promptly provide copies of any changes to its Red Flag policies and procedures. CONSULTANT shall comply with the City's red flag policy and report any Red Flags to the Program Administrator. Said report shall include Red Flags detected by CONSULTANT and CONSULTANT's response to the Red Flags so detected.

11. HIPAA Compliance. The software and services may include the storage or use of protected health information under Health Insurance Portability and Accountability Act (HIPAA). Therefore, CONSULTANT (for purposes of this section, "Business Associate") shall warrant that its software complies with HIPAA. CONSULTANT shall:

a. Not use or disclose protected health information other than as permitted or required by the agreement or as required by law;

b. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the agreement;

c. Timely report to City any use or disclosure of protected health information not provided for by the agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree, in writing, to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

e. Make available protected health information in a designated record set to the City as necessary to satisfy City's obligations under 45 CFR 164.524;

f. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the City pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy City's obligations under 45 CFR 164.526;

g. Maintain and make available the information required to provide an accounting of disclosures to the City as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

h. To the extent the business associate is to carry out one or more of City's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the City in the performance of such obligation(s); and

i. Make its internal practices, books, and records available to the Secretary and to the City for purposes of determining compliance with the HIPAA Rules.

12. Confidentiality. Both parties recognize that their respective employees and agents, in the course of performance of the agreement, may be exposed to

confidential information and that disclosure of such information could violate rights to private individuals and entities. Each party agrees that it will not disclose any confidential information of the other party and further agrees to take appropriate action to prevent such disclosure by its employees or agents. The confidentiality covenants contained herein shall survive the termination or cancellation of the agreement. This obligation of confidentiality shall not apply to (a) information that at the time of the disclosure is in the public domain; (b) information that, after disclosure, becomes part of the public domain by publication or otherwise, except by breach of the agreement by a party; (c) information that a party can establish by reasonable proof was in that party's possession at the time of disclosure; (d) information that a party receives from a third party who has a right to disclose it to that party; or (e) information that is considered an open public record pursuant to the Missouri Sunshine law.

13. Risk During Equipment / Software Storage and Installation. Delivery shall be made in accordance with the implementation schedule referenced as part of the agreement. Minor variances from this implementation schedule may be permitted subject to as mutual agreement by both parties and confirmed by prior written notice. During the time period where the equipment / software is in transit and until the equipment is fully installed in good working order, the CONSULTANT and its insurer shall be responsible for the equipment / software and relieve the CITY of responsibility for all risk or loss or damage to the equipment / software. In addition, CONSULTANT shall hold the CITY and its officers, employees and agents harmless from any risk of loss or damage arising out of occurrences during the installation of the equipment / software.

14. Shipping of Equipment / Software. All shipping and insurance costs to and from the site shall be included in the pricing. All payments to shipping agents and for insurance fees shall be made directly by the CONSULTANT. The CITY shall make no payments to any firm concerning the shipment, installation, and delivery of equipment / software which is not a part of the agreement and for which exact payments are not described. CONSULTANT shall be responsible for all arrangements for the shipment and receipt of equipment / software to CITY'S prepared site.

15. Ownership of Intellectual Property and Work Product. All information, data, programs, publications & media created specifically for and paid for by the CITY or as a result of the Work identified in the agreement is the property of the CITY unless otherwise noted, copyright protected, or defined or agreed to by both parties.

16. Insurance. CONSULTANT shall maintain, on a primary basis and at its sole expense, at all times during the life of this Agreement the following insurance coverages, limits, including endorsements described herein. The requirements

contained herein, as well as the CITY's review or acceptance of insurance maintained by CONSULTANT is not intended to, and shall not in any manner limit or qualify the liabilities or obligations assumed by CONSULTANT under this Agreement. Coverage to be provided as follows by a carrier with A.M. Best minimum rating of A-VI.

a. Workers' Compensation & Employers Liability. CONSULTANT shall maintain Workers' Compensation in accordance with Missouri State Statutes or provide evidence of monopolistic state coverage. Employers Liability with the following limits: $500,000 for each accident, $500,000 for each disease for each employee, and $500,000 disease policy limit.

b. Commercial General Liability. CONSULTANT shall maintain Commercial General Liability at a limit of $2,000,000 Each Occurrence, $3,000,000 Annual Aggregate. Coverage shall not contain any endorsement(s) excluding nor limiting Product/Completed Operations, Contractual Liability or Cross Liability.

c. Business Auto Liability. CONSULTANT shall maintain Business Automobile Liability at a limit of $2,000,000 Each Occurrence. Coverage shall include liability for Owned (if applicable), Non-Owned & Hired automobiles. In the event CONSULTANT does not own automobiles, CONSULTANT agrees to maintain coverage for Hired & Non-Owned Auto Liability, which may be satisfied by way of endorsement to the Commercial General Liability policy or separate Business Auto Liability policy.

d. CONSULTANT may satisfy the liability limits required for Commercial General Liability or Business Auto Liability under an Umbrella or Excess Liability policy. There is no minimum per occurrence limit of liability under the Umbrella or Excess Liability; however, the Annual Aggregate limit shall not be less than the highest "Each Occurrence" limit for either Commercial General Liability or Business Auto Liability. CONSULTANT agrees to endorse CITY as an Additional Insured on the Umbrella or Excess Liability, unless the Certificate of Insurance state the Umbrella or Excess Liability provides coverage on a "Follow-Form" basis.

e. The City of Columbia, its elected officials and employees are to be Additional Insured with respect to the Project to which these insurance requirements pertain. A certificate of insurance evidencing all coverage required is to be provided at least ten (10) days prior to the Effective Date of the Agreement between the CONSULTANT and CITY. CONSULTANT is required to maintain coverages as stated and required to notify CITY of a Carrier Change or cancellation within two (2) business days. CITY reserves the right to request a copy of the policy.

f. The Parties hereto understand and agree that CITY is relying on, and does not waive or intend to waive by any provision of this Agreement, any monetary limitations or any other rights, immunities, and protections provided by the State of Missouri, as from time to time amended, or otherwise available to CITY, or its elected officials or employees.

g. Failure to maintain the required insurance in force may be cause for termination of this Agreement. In the event CONSULTANT fails to maintain and

keep in force the required insurance or to obtain coverage from its subcontractors, CITY shall have the right to cancel and terminate this Agreement without notice.

h. The insurance required by the provisions of this article is required in the public interest and CITY does not assume any liability for acts of CONSULTANT and/or CONSULTANT's employees and/or CONSULTANT's subcontractors in the performance of this Agreement.

17. Conflicts. No salaried officer or employee of CITY and no member of City Council shall have a financial interest, direct or indirect, in this Agreement. A violation of this provision renders this Agreement void. Any federal regulations and applicable provisions in Section 105.450 et seq. RSMo shall not be violated. CONSULTANT covenants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of services to be performed under this Agreement. CONSULTANT further covenants that in the performance of this Agreement no person having such interest shall be employed.

18. Assignment. This Agreement shall inure to the benefit of and be binding upon the Parties and their respective successors and permitted assigns. Neither Party shall assign this Agreement or any of its rights or obligations hereunder without the prior written consent of the other Party.

19. Compliance with Laws. CONSULTANT agrees to comply with all applicable federal, state and local laws or rules and regulations applicable to the provision of services hereunder.

20. Employment Of Unauthorized Aliens Prohibited. CONSULTANT agrees to comply with Missouri State Statute section 285.530 in that CONSULTANT shall not knowingly employ, hire for employment, or continue to employ an unauthorized alien to perform work within the state of Missouri. As a condition for the award of this Agreement, CONSULTANT shall, by sworn affidavit and provision of documentation, affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services. CONSULTANT shall also sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. CONSULTANT shall require each subcontractor to affirmatively state in its contract with CONSULTANT that the subcontractor shall not knowingly employ, hire for employment or continue to employ an unauthorized alien to perform work within the state of Missouri. CONSULTANT shall also require each subcontractor to provide CONSULTANT with a sworn affidavit under the penalty of perjury attesting to the fact that the subcontractor's employees are lawfully present in the United States.

21. General Independent Contractor Clause. It is expressly agreed that the CONSULTANT is an independent contractor and not an agent of CITY. The

CONSULTANT shall not pledge or attempt to pledge the credit of CITY or in any other way attempt to bind the CITY. The relationship of the CONSULTANT to CITY shall be that of independent contractor; and no principal agent or employer-employee relationship is created by the contract.

22. Hold Harmless Agreement. To the fullest extent not prohibited by law, CONSULTANT shall indemnify and hold harmless the City of Columbia, its directors, officers, agents, and employees from and against all claims, damages, losses, and expenses (including but not limited to attorney's fees) arising by reason of any act or failure to act, negligent or otherwise, of CONSULTANT, of any subcontractor (meaning anyone, including but not limited to consultants having a contract with CONSULTANT or a subcontractor for part of the services), of anyone directly or indirectly employed by CONSULTANT or by any subcontractor, or of anyone for whose acts CONSULTANT or its subcontractor may be liable, in connection with providing these services. This provision does not, however, require CONSULTANT to indemnify, hold harmless, or defend the City of Columbia from its own actions, inactions, (willful or otherwise), or its own negligence.

23. No Waiver of Sovereign Immunity. In no event shall the language of this Agreement constitute or be construed as a waiver or limitation for either Party's rights or defenses with regard to each Party's applicable sovereign, governmental, or official immunities and protections as provided by federal and state constitution or law.

24. Professional Oversight Indemnification. CONSULTANT understands and agrees that CITY has contracted with CONSULTANT based upon CONSULTANT's representations that CONSULTANT is a skilled professional and fully able to provide the licenses and services set out in this Agreement. In addition to any other indemnification set out in this Agreement, CONSULTANT agrees to defend, indemnify and hold and save harmless CITY from any and all claims, settlements, and judgments whatsoever arising out of CITY's alleged negligence in hiring or failing to properly supervise CONSULTANT.

25. Professional Responsibility. CONSULTANT shall exercise reasonable skill, care, and diligence in the performance of its services and will carry out its responsibilities in accordance with customarily accepted good professional practices. If CONSULTANT fails to meet the foregoing standard, CONSULTANT shall perform at its own cost, and without reimbursement from CITY, the professional services necessary to correct the errors and omissions which are caused by CONSULTANT's failure to comply with above standard, and which are reported to CONSULTANT within one (1) year from the completion of CONSULTANT'S services for the Project.

26. Governing Law and Venue. This Agreement shall be governed, interpreted, and enforced in accordance with the laws of the State of Missouri and/or the laws of

the United States, as applicable. The venue for all litigation arising out of, or relating to this Agreement, shall be in Boone County, Missouri, or the United States Western District of Missouri. The Parties hereto irrevocably agree to submit to the exclusive jurisdiction of such courts in the State of Missouri. The Parties agree to waive any defense of forum non conveniens.

27. No Third-Party Beneficiary. No provision of this Agreement is intended to nor shall it in any way inure to the benefit of any customer, property owner or any other third party, so as to constitute any such Person a third-party beneficiary under this Agreement.

28. Notices. Any notice, demand, request, or communication required or authorized by this Agreement shall be delivered either by hand, facsimile, overnight courier or mailed by certified mail, return receipt requested, with postage prepaid, to:

If to CITY:	If to CONSULTANT:
City of Columbia	
Information Technology Department	Imagenet Consulting, LLC
ATTN: Mark Neckerman	ATTN: Contracts
P.O. Box 6015	913 North Broadway
Columbia, MO 65205-6015	Oklahoma City, OK 73102

The designation and titles of the person to be notified or the address of such person may be changed at any time by written notice. Any such notice, demand, request, or communication shall be deemed delivered on receipt if delivered by hand or facsimile and on deposit by the sending party if delivered by courier or U.S. mail.

29. Public Records Act. CITY is subject to the Missouri Sunshine Law. The Parties agree that this Agreement shall be interpreted in accordance with the provisions of the Missouri Sunshine Law as amended and CONSULTANT agrees to maintain the confidentiality of information which is not subject to public disclosure under the Sunshine Law.

30. Amendment. No amendment, addition to, or modification of any provision hereof shall be binding upon the Parties, and neither Party shall be deemed to have waived any provision or any remedy available to it unless such amendment, addition, modification or waiver is in writing and signed by a duly authorized officer or representative of the applicable Party or Parties.

31. Audit. CONSULTANT shall maintain financial records according to generally accepted accounting standards. CITY has the right, at its sole expense and during normal working hours, to examine the records of CONSULTANT to the extent reasonably necessary to verify the accuracy of any statement, charge or computation made pursuant to this Agreement.

32. Nondiscrimination. During the performance of this Agreement, CONSULTANT shall not discriminate against any employee, applicant for employment or recipient of services because of race, color, religion, sex, sexual orientation, gender identity, age, disability, national origin, or any other legally protected category. Consultant shall comply with all provisions of laws, rules and regulations governing the regulation of Equal Employment Opportunity including Title VI of the Civil Rights Act of 1964 and Chapter 12 of the City of Columbia's Code of Ordinances.

33. Missouri Anti-Discrimination Against Israel Act. To the extent required by Missouri Revised Statute Section 34.600 and not in violation of the state or federal constitution, CONSULTANT certifies it is not currently engaged in and shall not, for the duration of this Agreement, engage in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel. If any provision of this paragraph, or the application of such provision to any person or circumstance, shall be held invalid, the remainder of this Agreement, or the application of such provision to persons or circumstances other than those as to which it is held invalid, shall not be affected thereby. This paragraph shall not apply to contracts with a total potential value of less than one hundred thousand dollars ($100,000.00) or to contractors with fewer than ten (10) employees.

34. Patents, Copyrights, and Proprietary Rights Indemnification. The CONSULTANT, at its own expense, shall completely and entirely defend the CITY from any claim or suit brought against the CITY arising from claims of violation of United States patents or copyrights resulting from the CONSULTANT or the CITY's use of any equipment, technology, documentation, and/or data developed in connection with the services and products described in this Agreement. The CITY will provide the CONSULTANT with a written notice of any such claim or suit. The CITY will also assist the CONSULTANT, in all reasonable ways, in the preparation of information helpful to the CONSULTANT in defending the CITY against this suit. In the event that the CITY is required to pay monies in defending such claims, resulting from the CONSULTANT being uncooperative or unsuccessful in representing the CITY'S interest, or in the event that the CITY is ordered to pay damages as a result of a judgment arising out of an infringement of patents and/or copyrights, CONSULTANT agrees to fully reimburse the CITY for all monies expended in connection with these matters. The CITY retains the right to offset against any amounts owed CONSULTANT any such monies expended by the CITY in defending itself against such claims. Should a court order be issued against the CITY restricting the CITY'S use of any product and should the CONSULTANT determine not to further appeal the claim issue, at the CITY's sole option the CONSULTANT shall provide, at the CONSULTANT'S sole expense, the following: (a) Purchase for the CITY the rights to continue using the contested product(s), or (b) Provide substitute

products to the CITY which are, in the CITY'S sole opinion, of equal or greater quality, or (c) Refund all monies paid to the CONSULTANT for the product(s) subject to the court action. The CONSULTANT shall also pay to the CITY all reasonable losses related to the product(s) and for all reasonable expenses related to the installation and conversion to the new product(s).

35. Development Of Additional Applications Using Data. CONSULTANT shall provide access to data through an interface suitable to the need to allow CITY to develop additional applications using the data, to hire others to develop additional applications, to allow members of the public to develop additional applications, including but not limited to work for hire or a contest type event. CONSULTANT shall provide access to data to allow any such applications to utilize real time data. To allow for the functioning of any applications using Data through the API, CONSULTANT shall notify CITY in advance of any changes in the formatting of the API no later than seven (7) days prior to the change.

36. Control of Sub-Contractor, Project Team and Project Manager Designation. The CONSULTANT understands that the successful installation, testing, and operation of the system that is the subject of the agreement shall be accomplished by a cooperative effort. To most effectively manage this process, the CONSULTANT shall designate a single representative to act as an ex-officio member of the CITY'S project management team and who shall have the authority to act on behalf of the CONSULTANT on all matters pertaining to this Agreement. CITY shall have the right to approve all subcontractors, Account / Project Manager, and staff assigned to CITY by CONSULTANT. In the event that an employee of the CONSULTANT is, in the opinion of the CITY, uncooperative, inept, incompetent, or otherwise unacceptable, the CONSULTANT agrees to remove such person from the project. In the event of such a removal, the CONSULTANT shall, within fifteen (15) days, fill this representative vacancy as described above. Regardless of whom the CONSULTANT has designated as the representative, the CONSULTANT remains the ultimate responsible party for performing the tasks and responsibilities presented in the agreement.

37. Background Checks. If CONSULTANT's employees have access to the criminal justice information, background checks will be required.

38. Third party software. CONSULTANT warrants that all third party software products, brands, types, etc., have been recommended based on CONSULTANT's understanding of the CITY's operating environment and that such third party software products, brands, types, etc., shall operate as demonstrated by CONSULTANT and as documented in documentation. CONSULTANT warrants that they have the right to license said third party software products, brands, types, etc.

39. Warranty. The CONSULTANT warrants that all components provided under the agreement, whether installed initially or under subsequent purchase orders, shall be: newly manufactured equipment or assembled from newly manufactured parts; approved by Underwriter's Laboratories; and, will be free from defects in workmanship or material for a period of 12 months (365 calendar days) from the date of final system acceptance. During this 12 month warranty period, the CONSULTANT shall furnish all replacement new parts, shipping costs, repaired parts, service labor, travel costs, and other repair costs at no cost to the CITY. At the conclusion of the warranty period, the CITY may consider Consultant support under a separate maintenance agreement.

40. Warranty of Fitness for a Particular Purpose. CITY has presented detailed technical specifications of the particular purpose for which the technology is intended. Given this advanced preparation, and documentation about the CITY's particular purpose, the CONSULTANT acknowledges at the time this Agreement is in force that CONSULTANT has (1) reason and opportunity to know the particular purpose for which products are required, and (2) that the CITY is relying on the CONSULTANT's experience and knowledge of these products to provide those which are most suitable and appropriate. Therefore, CONSULTANT warrants that the system is fit for the purposes for which it is intended as described in CITY's Request For Proposal.

41. Continuity of Warranty. CITY may continue the Warranty protection described above by purchasing and paying for on-going Annual Support services. By doing so, all Warranty, Warranty of Fitness for a Particular Use, and Resolution and Response Time Warranty conditions above shall remain in effect (except for the "Third party hardware" clause above), as long as payments for Annual Support are kept current.

42. Final Acceptance of the System. The system proposed shall be defined to be finally accepted by CITY after the installation of the equipment, training, and successful completion of the following performance examinations: system hardware examination, software performance examination, system functional competence examination, system capacity examination, full-load processing capacity examination, system availability examination, approval of as-builts, training, and system documentation. The CITY shall be the sole judge of whether all conditions for final acceptance criteria have been met.

43. Password Security. The CONSULTANT warrants that no 'back door' password or other method of remote access into the software code exists. The CONSULTANT agrees that any and all access to any software code residing on

the CITY'S server must be granted by the CITY to the CONSULTANT, at the CITY'S sole discretion.

44. Non-Performance Escalation Procedures. In the event that the CITY determines that CONSULTANT is not performing in a manner consistent with the intent and spirit of the agreement or in a manner consistent with commonly accepted business practices, then the CITY shall have the right to, in the sequence shown: (a) formally notify CONSULTANT of non-performance, (b) reserve the right to withhold any and all payments pending, including support and maintenance agreement fees, until the non-performance is corrected, (c) request a joint meeting of CONSULTANT and CITY decision makers to attempt to resolve the non-performance, (d) require a CONSULTANT employee to be on-site at CITY'S location until the non-performance is resolved, or (e) invoke the Termination clause herein.

45. Nature of City's Obligations. All obligations of the CITY under this Agreement, which require the expenditure of funds, are conditional upon the availability of funds budgeted and appropriated for that purpose.

46. Travel Expense Reimbursement. All travel expense costs must be included in the CONSULTANT'S fixed price cost. CITY will not make a separate payment for reimbursable expenses. CITY shall not be liable for additional travel costs incurred due for any reason outside CITY'S control.

47. Video Taping. CITY reserves the right to video and/or audiotape any and all training sessions, whether held at CITY site, CONSULTANT'S site, or via teleconference or webinar. Use of such tapes shall be strictly for CITY staff training purposes.

48. Major Releases / Upgrades. CITY shall be entitled to future releases and upgrades within five (5) years from Formal Acceptance, whether of a "minor" or major" nature, of Laserfiche Software for no additional cost beyond the Annual Support fees. Professional service time spent by CONSULTANT on upgrades would have a cost associated.

49. Solution Longevity. The CONSULTANT certifies solutions prescribed in their proposal response will remain available and supported for a minimum of five (5) years from the time the contract is signed and that any material changes to CONSULTANT'S company or products will not affect the CITY'S implementation or support.

50. Counterparts and Electronic Signatures. This Agreement may be signed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. Faxed signatures, or scanned and electronically transmitted signatures, on this Agreement or any notice delivered pursuant to this Agreement, shall be deemed to have the same legal effect as original signatures on this Agreement.

51. Contract Documents. The Contract Documents include this Agreement and the following attachments and exhibits which are incorporated herein by reference.

Exhibit:

A	Scope of Services
B	Schedule of Work
C	Pricing Sheet
D	CITY's Red Flag Policy
E	Service Level Agreement

In the event of a conflict between the terms of any of the Contract Documents and the terms of this Agreement, the terms of this Agreement control. In the event of a conflict between the terms of any Contract Documents, the terms of the documents control in the order listed above.

52. Entire Agreement. This Agreement represents the entire and integrated agreement between the Parties relative to the Project herein. All previous or contemporaneous contracts, representations, promises and conditions relating to CONSULTANT's services on this Project described herein are superseded.

[SIGNATURES ON FOLLOWING PAGE]

IN WITNESS WHEREOF, the Parties hereto have set their hands on the day and year written below.

CITY OF COLUMBIA, MISSOURI

By: _____

Name: De'Carlon Seewood

Title: City Manager

Date: _____

APPROVED AS TO FORM:

By: _____
Nancy Thompson, City Counselor/rw

CERTIFICATION: I, hereby certify that this Agreement is within the purpose of the appropriation to which it is to be charged, Account Number 44008810-604990-00850, and that there is an unencumbered balance to the credit of such appropriation sufficient to pay therefor.

By: _____
Director of Finance

(Seal)

Imagenet Consulting, LLC

By: _____

Date: 10-4-22

ATTEST:

By: _____

Name: _____

EXHIBIT A

Scope of Services

PROJECT OBJECTIVES

- Establish a single repository for documents
- Streamline existing processes and increase productivity
- Increase integration and interaction between departments
- Improve workflow processes to streamline movement of documents between staff and departments to improve customer service
- Reliable and accurate results when searching documents stored in the DMS (advanced Optical Character Recognition (OCR) technology)
- All users will interact directly with the DMS to either enter/track their existing paper or retrieve documents as needed from other departments
- Reduce liabilities through effective management of multiple types of documents (scanned or electronically generated), and improving the tracking, retrieval, retention, and final disposition of these documents
- Share documents in both a structured and ad-hoc manner across the organization
- Quickly and easily provide accurate information for Sunshine requests

The City is seeking solutions that offer the following attributes:

- System integrations with Tyler Technologies, LLC Munis and EnerGov ERP systems
- System reliability
- System flexibility
- System scalability
- System interoperability
- System integrity – data security and user access levels
- System user defined parameters

The proposed solution must focus on the need the City of Columbia has to consolidate and improve records management, retention, indexing, workflow, document access and retrieval of documents created and utilized by City staff. The system shall store digital images quickly and effectively for later retrieval by securely defined user or group access.

The solution must interface with Tyler Technologies, LLC products (Munis, Energov, Tyler 311, DHD and Mobile Eyes).

The system shall support archival permanency with the ability to migrate records to other mediums (hardware or software) for the full retention of a record and be able to remove records by date, type or number range. The system must be able to export the digital information into various formats, and to allow quick, easy, and timely retrieval of records and information as needed. The system must have the ability to control the authoring, check in/out, and/or version control of documents being developed, managed or stored. It shall also give users the ability to index or enter the "metadata" associated with the documents being entered into the system. Migrating existing data from multiple systems will be required.

The DMS solution must be scalable to support the inclusion of the City's existing data from FileBound

and TCM and allow additional electronic and paper documents to be scanned and imported. In general, users need fast retrieval of information and search tools to locate information. Workflow solutions to efficiently process and route documents are being considered. Additionally, users need a faster method to attach, save and relate documents in Tyler Technologies software products. The City is also looking to take existing paper documents that will be archived for a specified period of time and scan them into a document management system. The system shall include document imaging, management, indexing, searching (advanced OCR capabilities), inline editing, and document archiving/retention.

The proposed document management system shall be specifically designed for heavy-duty municipality use. The DMS shall incorporate the latest technology available at the time of installation and must be easily upgradeable when hardware/software improvements become available.

Proposed solutions must include the following elements:

- Application software
- Software implementation
- Data Migration (in partnership with City's IT Department)
- Computer hardware and setup
- System interfaces
- Comprehensive Testing / Proof of Concept Statement of Work
- Software and hardware maintenance
- Project management (in partnership with City of Columbia's Project Management Office)
- Comprehensive training

TECHNICAL SPECIFICATIONS:

The City requires the solution to be configurable for one (1) production environment and four (4) non-production environments, including a procedure or process to sync data from production to any non-production environment.

The solution and data may remain on premises in the City's secured datacenter or the solution data may be hosted externally as long as the hosting requirements (Attachment 1) are met and application performance is acceptable.

DOCUMENT TYPES

Given the wide ranging interests in document management technologies it is not surprising to see that the types of documents that may go into a central repository are quite extensive. Examples of documents that would be considered for this system include, but are not limited to:

• Agreements • Audit reports • Background checks • Bonds • Budget documents • Building Plans • Business License Documents • Board Actions • City Council Documents • Certificates • Contracts and Amendments • Correspondence • Diagrams • Drivers License • Electronic mail • Employee Documentation • Faxes • General notes/minutes	• Grant proposals • Invoices / Quotations • Insurance Documents/Letters • License agreements • Memos • Misc/Other • Paychecks • Permits • Personnel actions • Photographs • Presentations • Project plans • Proposals • Purchase Orders • Reports/papers • Spreadsheets • Word processing documents • Vendor files

Documents handled by a typical department include, but are not limited to: 8 ½" x 11", 8 ½" x 14", or 11 x 17" in size, and can include both printed and handwritten text. These documents can be both single/double-sided; they can be folded, stapled, wrinkled, faded, and odd-size documents (e.g., post-it notes or very large pages such as blueprints). Document types include, but are not limited to: TIF, PDF, JPG, GIF, Microsoft Office standard formats such as .docx and .xlsx. Scanned documents can be large (exceeding 2 GB) and several hundred pages in length.

HARDWARE

City applications are accessed via desktop computers and laptops. The city standard for information technology equipment is outlined below. The following table summarizes the City's current Information Technology standards:

Standard / Guideline	Objectives / Characteristics
Client Workstation	◊ IBM-compatible PC with MS Windows Win 10 ◊ Antivirus: Trend Micro Apex One 2019 ◊ Browser: Chrome, FireFox, IE v11 or above ◊ PDF: Adobe Acrobat Reader ◊ Email: Google ◊ Google Suite and Microsoft Office 2017
Server Hardware	◊ Virtual Infrastructure: VMWare ESXi

	◊ Windows Server 2016/2019 ◊ Active Directory Compliant
Database Management	◊ Microsoft Windows 2017 Standard ◊ SQL Server 2017/2019 Standard
Network Operating System / Connectivity	◊ TCP/IP compliant ◊ Microsoft Active Directory Domain
Document Transfer (EDI)	◊ Compliance with X12 ANSI standards
Reporting	◊ Crystal Reports ◊ SSRS (SQL Server Reporting Services) ◊ PowerBI
Scanners	◊ Canon DR-2580C ◊ Canon DR-M140 ◊ EPSON DS-510 ◊ EPSON ES-400
Multi-Function Printers (optional)	◊ CANON / Image Runner C5235 ◊ CANON / iR-ADV C9280-A2 ◊ HP Color LaserJet M750 ◊ HP Color LaserJet MFP 400 ◊ HP Color LaserJet MFP M476dn ◊ HP Color LaserJet MFP M570DN ◊ HP Color LaserJet MFP M680 ◊ HP LaserJet M630 ◊ HP LaserJet M652dn ◊ HP Laserjet MFP M4345 ◊ HP LaserJet MFP M4555 ◊ HP Laserjet MFP M830z ◊ Sharp MX-3071 ◊ Sharp MX-4071

	◊ Sharp MX-4072 ◊ Sharp MX-B476W ◊ Sharp MX-M3071 ◊ Sharp MX-M3571 ◊ Sharp MX-M4071

Exhibit B – Schedule of Work

For

City of Columbia

10/17/2022
SOW Valid For 60 Days After This Date

Proposal

City of Columbia has engaged ImageNet Consulting to work with their staff to design and implement a digital and automated system to address their critical business objectives in a dynamic nature through the engagement of an Integrated Resource (IR). This document is intended to set expectations for efforts associated with implementing strategic change. Long term strategic vision built through the efforts described herein shall provide guidance to current and future transformation engagements.

The purpose of this IR is to work with the city staff both in IT and across all impacted divisions to instantiate an instance of the Laserfiche software suite. The original intent of the RFP put out by the city was focused on design and implementation of Laserfiche as an alternative and superior solution to current document and workflow systems in place today. Alongside that endeavor and this IR is the intake and reorganization of data that has been migrated out of both FileBound and Tyler CM by city IT staff. This migratory component will be presented separately in a Not-To-Exceed priced offering.

Beyond these core objectives along with all the ancillary activities around that such as integration into multiple Tyler systems; Munis (Using LF Connector) and Energov (Using ECS Imaging Connector), the objective of every IR is to work with the City of Columbia staff to wholistically over the course of this engagement to develop vision and roadmap for long-term strategic growth of their organization through the functions and features at their disposal through the Laserfiche Software Suite.

Once the core foundational aspects of the systems are in place as well as designated staff within the city being trained to a level of sufficient expertise, remaining time can be used to continue to either develop roadmap strategy or rollout of development/deployment to various processes/departments in the City as directed and prioritized by City representatives.

As a reminder, the benefit of an IR is to provide a temporal engagement for an imbedded resource with full focus on the success and growth of the City environment for this 90 day engagement, however because this is a temporal engagement it is critical that this resource be utilized at all times and responses and activities be structured to not leave idle time. Also, it needs to be understood that while a large part of this is the visioning strategy for long-term development that it doesn't necessarily result in all possible roadmap objectives being completed within the allotted time frame. Rather that instead of a stream of change orders and activity delays that the financial governance and outcome of this engagement is returned to the City as it would be with any staff on their direct payroll.

Strategic Change

Based on available information, a phased approach is recommended to reach an ideal future state, initially focusing on high level understanding of the current state and challenges the organization faces leading to a roadmap, laying the foundation with guidance for adaptive change and continual value realization over time. This approach will provide the organization with the opportunity to adjust to changes, learning from them throughout the change and adapting without losing focus on the holistic and strategic goals of the organization's long-term future. Following is a high-level phased approach, focusing on minimum needed to experience continual improvement and value over time.

Transformational Approach

Phase I:

Visioning, Strategy, and Process Literacy

Phase II and Beyond:

Incremental implementation of a roadmap and digital foundation as defined in Phase I, allowing for adaptive change based on new business needs and learnings.

Through the strategic use of integrated resources, this allows for a holistic solution to be developed, creating a centralized and efficient flow of documents, data, and processes in order to further the mission of the organization. Scope of Phase I can be limited to a specific department or it can be done at a larger organization level that allows City of Columbia ability to discern the desired location for starting Phase II within their organization.

System Implementation Details

Licensing for Laserfiche has been procured and established in a separate document or a previous engagement. Should any new modules or licenses be identified as necessary they will need to be quoted and addressed at that point.

Scheduling Details

Due to the fluid nature of project scoping, SOW review, project negotiation, and other factors, scheduling for projects cannot be set until project documents are signed and contracts are in place. The following factors stand:

- Project Kick-Off meeting with client staff and ImageNet representatives will occur, or be scheduled, within 10 days of contractual agreement. (Dependent on client availability)
- Client understands that as part of lean process environment, ImageNet resources are typically booked out ahead of time at minimum 10-12 weeks and, aside from the kick-off meeting, projects will most likely not begin before that time frame. With the nature of extended integrated engagements times may push out further based on renewals of existing engagements. Resources must be cleared of any remaining project work to ensure full dedicated availability.

Phased Approach to the Future Environment

Phase I: Visioning, Strategy, and Process Literacy

- Visioning
  - Initial engagement to solidify a vision and strategic approach for transformation
  - provide the foundations for successful process literacy, which in turn sets the stage for transformative success
- Process Literacy
  - Building visual and textual aids to create mutual understanding of process, data, culture, and its respective sources and destinations.
  - Perform process analytics to derive meaningful insight into the requirements, quality and appropriate implementation of client processes
- Work Products
  - Process scoping - high level documentation of identified objective implementations within organization
  - Business case for identified phase two objectives - detailed documentation and narrative for the value proposed to be gained in phase II implementations. This can become the guiding light for ongoing transformation engagements.
  - Process Diagrams - Forms, diagrams, and graphical representations of processes and data flows containing both source and destination as well as the meaning and purpose.

Phase II: Incremental Transformation and Foundation Establishment

- Actualization of engagements driven by business case and other documentation defined in phase one
- Executing change in incremental phases once an agreed upon foundation is in place, providing consistency and value as a result.
- Quality assurance of each objective, including documentation and training.
- Guided transformation from current to future state to include careful consideration of data, documentation, process, client culture, and technology for successful change.

Investment and Scope

Investment

During this engagement, all efforts will be made by all parties to continually engage and progress in the change initiative, working through the phases mentioned above. Terms associated with engagement can be found in The Rules for Success section of this document. Throughout the engagement, if additional resources or skills are needed and/or desired, addendums to this document can be defined and agreed upon.

Services Included

During this engagement, all efforts will be made by all parties to continually engage and progress in the change initiative.

Service	Description
Consulting / Analysis	Collaborate to ensure goals and deliverables for the immediate change desired are well understood. If this is performed by an ImageNet partner, this element may not be necessary
Development / Implementation	Technical activities to execute on processes and data elements defined in consulting and analysis efforts.
Long Term Transformation Strategy	Time permitting and when appropriate, engage in follow-up analysis and vision definition to determine the next logical business process of value to be delivered.
Training	Educational engagement enabling client staff to utilize applications put in place with optimal efficiency. Training of available technical or super-user staff, enabling client to be self-sufficient in maintaining and further developing the system to the highest level of success possible.

Pricing

Item	Qty	Monthly Rate	Term	Total
Integrated Resources* *Monthly Equivalent Part Time Remote "employee(s)"; supporting resources are provided as appropriate max 18 hours/week	6	15,940.00	6 Month Term Minimum	$ 95,640.00
Consulting/Analysis (beyond initial Period included in Term)	0	225.00	None	N/A

Milestones

Item	Description
Overall Period	Overall Timeframe for engagement. If additional detail is appropriate for specific activities, such will be found below
Consulting / Analysis	Early efforts to define the roadmap of change associated with the implementation efforts as well as requirements for the immediate change at hand
Development/ Implementation	Efforts to build and implement the solutions designed in the previous phase of change
Walkthrough and Design Acceptance	Review and walkthrough of the completed design with time for non-foundational revisions. Final design acceptance in preparation for Go-Live
Training	Coordinated training periods with client staff to review the product function as well as specific designs implemented and accepted in previous phases
Go-Live	Client staff using the newly developed system with limited oversight and high availability to the integrated resource to ensure any issues or assistance needs are quickly met. This will dramatically improve adoption and minimize negative impact to process.

Assumptions and Constraints

Type	Title	Title
Assumption	Resource Availability	Timeframe defined is dependent upon all resources having availability to review and act in a timely manner
Assumption	Scope	The immediate scope of Phase I is limited to high level understanding of challenges, structure, and focus priority
Assumption	Timeline	The timeframes provided are linear as an uninterrupted contract through final expiration of term

Risks

Type	Description	Mitigation
Resource availability	Lack of resources could reduce value output	Engage additional resources, when necessary. This would require a Change Request (CR).
Scope Creep	Defined need may be challenged during development	Leverage analyst skillset to challenge any changes and evaluate necessity. This would require a CR
Timeline	The defined timeframe may be challenged if other assumptions prove false	Ensure expectations and communications are clear with proactive discussion regarding perceived threats to timeline

Resources

Role	Name(s)	Responsibility	Contact Info
Lead Analyst	TBD	Collaborate with Client to accurately define vision and roadmap	
Project Manager	Simon Adeniji	Proactively engage ImageNet and Client resources ensuring progress	sadeniji@imagenet.com
Designer	TBD	Implement agreed upon road map and deliver training to users and administrators	
Account Executive	Caleb Swaringim	Manage overall account relationship and expectations	cswaringim@imagenet.com
Client SME	TBD	Provide process and organization structure as well as data and documentation. Critical role for enabling successful change	
Client Technical Resource	TBD	Client technical resource for any configuration or accessibility issues	
Client Primary Stakeholder	Sophie Heidenreich	Primary decision maker for final user acceptance phases	sophie.heidenreich@como.gov

Rules for Successful Engagement

RATE GUARANTEE
This rate is guaranteed through the calendar year and the initial term. Furthermore, it will not increase by more than 10% year over year if at all.

MONTHLY RECURRING SERVICES SUBSCRIPTIONS
The Service Plan will automatically renew thirty (30) days prior to the end of the engagement period for additional one-month terms at the then-current monthly rate per resource for those resources identified until the SP is terminated with thirty (30) days' written notice.

TERMINATION
Termination for any reason whatsoever is effective thirty (30) days following written notice to ImageNet.

RESOURCE AVAILABILITY
Team members PTO is included during time periods. For planned absences, Client shall be notified a minimum of two weeks in advance of such absence. Should a resource be unavailable for a significant time period, a secondary resource may be brought into the engagement to replace the unavailable resource. ImageNet will notify Client of the situation and options before engaging the new resource.

INVOICE PROCEDURES
Invoices will be generated and sent to Client at the beginning of each month. Payments for services invoiced are due based on the agreed terms in the PSA and SLA. Recurring Services and software subscription fees will be invoiced monthly. Travel expenses will be billed at cost, as incurred.

OUT-OF-POCKET EXPENSES
Client will be invoiced monthly all costs associated with out-of-pocket expenses (including, without limitation, costs and expenses associated with meals, lodging, local transportation and any other applicable business expenses) listed on the invoice as a separate line item. Such expenses will be reasonable and communicated and approved in advance of incurrence.

CHANGE CONTROL PROCEDURE
The following process will be followed if a change to this plan is required:
A Change Request (CR) will be the vehicle for communicating change. The CR must describe the change, the rationale for the change, and the effect the change will have on the engagement.

- The requesting party (ImageNet or Client) will review the proposed change with appropriate resources to determine value and, if the value is appropriate, submit the CR to the Project Managers of impacted organizations.
- Appropriate parties will review the impact of the proposed change and, if mutually agreed, the CR must be signed by both parties to authorize implementation of the requested change.

Client Responsibilities

Type	Contact Info
Staff Resources	Client to identify and provide an IT Administrator for solution implementation and support interaction.
Staff Resources	Client will provide an onsite primary contact person responsible for providing direction and approvals on completion of work.
Accessibility	Client will provide access to all areas required to complete this project. Any areas of high security or hazard should be made known prior to project commencement.
Accessibility	Client will provide access to all information and documentation required to complete this project.
Accessibility	Client will provide Remote Access capabilities and credentials so that ongoing support can be provided as necessary via phone and remote desktop support.
Accessibility	Client will assure that all required LAN/WAN access and administrative rights are made available to complete the installation.
Systems	Client will directly provide all non-ImageNet hardware and software support required unless specifically indicated otherwise and assure that all hardware meets required specifications.
Systems	Client will verify final and ongoing maintenance and user setup.
Systems	Client is solely responsible for back-up of any systems and databases present within their network and hardware, including application data. ImageNet maintains no backups.
Systems	Client will be responsible for all non-application related system setup, configuration, resources, and functions. Servers must operate on a currently supported Microsoft Windows environment.
Timeline	Client is responsible for providing access and maintaining agreed upon timeline. ImageNet staff may be idled as a result of delays. If significant delays are encountered during the service efforts outside of ImageNet's control, a re-engagement fee of $2,500.00 will be charged prior to ImageNet reengaging. For integrated Resources the reengagement fee will be a total of 1 week (1/4 monthly rate) for resource reallocation time.

Change Requests

If any changes or additions are required outside of the defined scope and deliverables previously listed, a Project Change Order Request will need to be completed and signed by both the Client Project Manager and ImageNet Consulting representatives. (Copy attached)

Assumptions & Terms

- Rates are based on a commitment that work is to be performed during regular business hours; 8AM to 5PM local time, Monday through Friday
- It is assumed that all work will be completed as a continuous effort. Disruptions of this continuous effort beyond the control of ImageNet Consulting may require additional costs, additionally if the project is finished ahead of the estimated completion, there will be no credit issued to the client.
- All System Engineer work outside of the work defined within the proposal is billed accordingly to SLA in place
- All Process Analyst work outside of the work defined within the proposal is billed accordingly to SLA in place
- For a full Professional Service Agreement, see MSA.

Exhibit B-Attachment A: Project Change Request

Project Change Request

PCR Number: _____

Date: _____ Party requesting change: _____

Nature of the proposed change:

_____
_____
_____

Reason for the proposed change:

_____
_____
_____

Impact of the proposed change on project:

Pricing: _____

P.O. to which changes will apply: _____

Schedule Changes:

_____
_____

This Project Change Request is (circle): Approved Rejected

Signatures:

ImageNet Consulting Representative: _____

Client Representative: _____

EXHIBIT C
PRICING SHEET

Implementation,Migration and Integration Services - ($186,640)	
Integrated and Dedicated Implementation Resource - 90 days	$95,640.00
Migrating City's Existing Data and Metadata to the new DMS (One time fee)	$70,000.00 NTE (Not to Exceed)
Optional Tyler Energov Integration	$21,000.00
Annual Subscription and Maintenance	
Complete Document Management System Subscription	$66,225.00 (Years 1-5)
Optional Tyler Energov Integration Maintenance	$2,400.00 (Years 2-5)
Admin Users Per month	$0.00 - ImageNet does not charge extra for admin users. Admins can use full user licenses.

YEAR ONE TOTAL: $252,865

YEARS 2-5 TOTAL: $274,500 ($68,625 ANNUALLY)

TOTAL FOR FIVE YEARS: $527,365

Exhibit D

CITY's Red Flag Policy

2010
Red Flag Rule

City of Columbia Identity Theft Prevention Program

Effective December, 2010

City Council Adopted and Effective Date: 12/6/10

This document is intended to give guidance to the City in their understanding of the FTC Red Flag Rule. It is not intended to be used in place of compliance, in whole or any part, of the FTC Rule.
08/02/10 Final
11/10/10 Reviewed/Updated

Table of Contents

INTRODUCTION

The City of Columbia (the "City") has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. §681.2. This Program is designed to detect, prevent and mitigate identity theft not only in connection with the opening and maintenance of City utility accounts but other city accounts, applications, registrations or other transactions, referred to as "Record" or "Records" throughout this Program, where identity theft might occur.

Why did FTC make this rule?
The intent is to protect consumers from identity theft. It is targeted at entities that **obtain** and **hold** consumer identification such as billing addresses, Social Security Numbers, dates of birth, passports or immigration documents, or other information.

Who must comply?
Entities such as Columbia that obtain and hold identification often targeted by identity thieves must comply.

What is a "Red Flag?"
A "Red Flag" is a term the FTC has coined to identify possible identity theft. It is a pattern or particular specific activity that indicates the possible risk of identity theft. The FTC has identified thirty-one "Red Flags" that entities, especially utilities, should watch for. Such entities are required to have a written plan to help employees identify these "Red Flags" and how to respond when a possible identity theft has occurred.

How does Columbia have to comply with this rule?
We have a duty to:

1. Identity Red Flags
2. Detect Red Flags; and
3. Respond to Red Flags

Who within City operations has to comply with the rule?
All City Departments which obtain and hold any of the consumer identification mentioned above must comply with the rule.

For purposes of this Program, "Identity Theft" is considered to be "fraud committed using the identifying information of another person." The Program "Record" is defined as:

1. A continuing relationship the City has with an individual through a Record the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account, registration, application or record the City offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the City from Identify Theft

This Program was developed with oversight and approval of the Columbia City Council. After consideration of the size and complexity of the City's operations and various systems, and the nature and scope of these activities, the Columbia City Council determined that this Program was appropriate for the City and therefore approved this Program on December 15, 2008.

The Red Flag Rule-City of Columbia Identity Theft Prevention Program was reviewed and amended December, 2010.

IDENTIFICATION OF RED FLAGS

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the City of Columbia considered risk factors such as the types of Records it offers and maintains, the methods it provides to open or establish these Records, the methods it provides to access its Records, and its previous experiences with Identity Theft. The City identified the following Red Flags in each of the listed Categories:

1. **Notifications and Warnings from Consumer Reporting Agencies**

   1) A fraud or activity alert that is included with a consumer report;

   2) Receiving a report or notice from a consumer reporting agency of a credit freeze;

   3) Receiving a report of fraud with a consumer report; and

   4) Receiving indication from a consumer report of activity that is inconsistent with a customer's usual pattern or activity.

2. **Suspicious Documents (see below) used in such a way (items 1-13)**

   - Lease
   - Death certificate
   - Driver's license
   - Immigration Papers or Work Card
   - Passport
   - Birth certificate
   - Student Identifications
   - Government Issued Identification
   - Military Identification
   - Non-Driver's License Identification
   - Credit and Debit Cards

   1) Receiving documents that are provided for identification that appear to be forged or altered;

   2) Receiving documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation;

   3) Receiving other information on the identification not consistent with information provided by the person opening a new Record or customer presenting the identification;

4) Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged);

5) Receiving an application for service that appears to have been altered, forged or gives the appearance of having been destroyed and reassembled;

6) Personal identifying information provided is inconsistent when compared against external information sources used by the Department (such as the address does not match any address in the Consumer Report or the Social Security Number has not been issued, or is listed on the Social Security Death's Master File);

7) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal knowledge and/or external third party sources (telephone number or address on an application is the same as the telephone number or address provided on a fraudulent application;

8) Receiving verbal, written, or internet based information where the same person with the same billing information requests utility service at more than one location;

9) The Social Security Number provided is the same as that submitted by other person(s) opening a Record;

10) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening Records;

11) The person opening a Record fails to provide all required personal identifying information (incomplete application);

12) The person opening a Record cannot provide authenticating information if requested to do so;

13) The Department is notified by a customer (s) with information that another customer may have opened a fraudulent Record.

3. Suspicious Personal Identifying Information

1) A person's identifying information is inconsistent with other sources of information (such as an address not matching an address on a Consumer Report or a Social Security Number that was never issued);

2) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent Social Security Numbers, billing addresses or birth dates);

3) A person's identifying information is the same as shown on other applications found to be fraudulent;

4) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or a fictitious billing address);

5) A person's Social Security Number is the same as another customer's Social Security Number;

6) A person's address or phone number is the same as that of another person;

7) A person fails to provide complete personal identifying information on an application when reminded to do so; and

8) A person's identifying information is not consistent with the information that is on file for the customer.

9) The physical appearance of a customer does not match with other sources of information (such as driver's license, passport or immigration work card).

10) A person does not know the last 4 digits of his/her Social Security Number.

11) A new customer requests new service and a routine Social Security Number check locates an account with delinquent or a collection balance that is proved not to be the responsibility of the customer requesting new service.

4. Unusual Use Of or Suspicious Activity Related to a Record

1) A change of address for a Record followed by a request to change the Record holder's name or add other parties;

2) A new Record used in a manner consistent with fraud (such as the customer failing to make the first payment, or making the initial payment and no other payments);

3) A Record being used in a way that is not consistent with prior use (such as late or no payments when the Record has been timely in the past);

4) Mail sent to the Record holder is repeatedly returned as undeliverable;

5) The Department receives notice that a customer is not receiving his paper statements; and

6) The Department receives notice that a Record has unauthorized activity.

7) A Record is designated for shut-off due to non-payment and the customer at the location does not match the customer on file.

8) Unauthorized access to or use of customer records information such as log on or authentication failures.

5. Notice Regarding Possible Identity Theft

The City receives notice from a customer, an identity theft victim, law enforcement or any other person that it has opened or is maintaining a fraudulent Account for a person engaged in Identity Theft.

DETECTION OF RED FLAGS.

1. **In order to detect any of the Red Flags identified above with the opening of a new Record, City personnel will take the following steps and verify the identity of the person opening the Record:**

    1) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, Social Security Number, driver's license or other identification;

    2) Verifying the customer's identity in person, such as by copying and reviewing a driver's license or other identification card;

    3) Reviewing documentation showing the existence of a business entity (in person process);

    4) Independently contacting the customer; and

    5) Requesting the customer to appear in person with appropriate information or documentation.

2. **In order to detect any of the Red Flags identified above for an existing Record, City personnel will take the following steps to monitor transactions with such information:**

    1) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email);

    2) Verifying the validity of requests to change billing addresses;

    3) Verifying changes in banking information given for billing and payment purposes; and

    4) Verifying the last 4 digits of his/her Social Security Number.

PREVENTING AND MITIGATING IDENTITY THEFT

1. **In the event City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:**

   1) Continuing to monitor a Record for evidence of Identity Theft;

   2) Person who may be or is suspected to be the possible victim of identity theft;

   3) Changing any passwords or other security devices that permit access to Records;

   4) Reopening a Record with a new number;

   5) Not opening a new Record;

   6) Closing an existing Record;

   7) Notifying law enforcement; See **Appendix D.**

      Example: If the City receives notice that its system has been compromised such that a customer's personal information has become accessible, at a minimum the City will notify the customer and change passwords.

      Example: If the City receives notice that a person has provided inaccurate identification information, the Record will be closed immediately and notify Law Enforcement.

   8) Determining that no response is warranted under the particular circumstances; or

      Example: If the City notices late payments on a Record regularly paid and determines the resident has been incapacitated, no action may be necessary.

   9) Notifying the Program Administrator for determination of the appropriate step (s) to take.

2. **In order to further prevent the likelihood of identity theft occurring with respect to Records the City will take the following steps with respect to its internal operating procedures:**

   1) Providing a secure website or clear notice that a website is not secure;

2) Ensuring complete and secure destruction of paper documents and computer files containing customer information. Paper documents and computer files containing customer information should be retained for the minimum retention required by law, unless there is a significant business purpose to retain the record for a longer period of time.

3) Requiring certain provisions included in city contracts with vendors. If the storage or destruction of paper documents and computer files are contracted to a private vendor, contracts must include a provision that requires the private vendor to store the documents and files in a secure manner so as to be accessible only by approved city personnel. Upon appropriate authorization by an approved city official, the vendor shall destroy the documents and computer files in a secure fashion. The storage and destruction of paper documents and computer files which contain sensitive information must be performed by either a city employee or a private vendor under contract.

4) Ensuring that office computers are password protected and that computer screens lock after a set period of time;

5) Requiring only the last 4 digits of Social Security Numbers on customer Records;

6) Requiring each Department review, no less than once a year, employee's access to Record information to determine if the employee's duties require such access and if the employee is complying with the provisions of the City Identity Theft Prevention Program. The Department shall restrict access as much as feasible and maintain an up to date list of those employees required to have access along with the date access was last reviewed. If the employee's access involves computer files, access shall be documented in the City Security Tracking System.

7) Prohibiting Record information to be written on sticky pads or note pads;

8) Ensuring that computer screens are only visible to the employee accessing the Record;

9) Requiring customers to authenticate addresses and personal information, rather than account representatives asking if the information is correct;

10) Maintaining secure office location;

11) Maintaining cameras in timely and good working order and providing for property destruction of tapes and other recording media;

12) Periodically (each Department) reviewing and maintaining a complete, accurate, and current internal list of authorized personnel and procedures with respect to the appropriate responses should a red flag occur or should the Department be aware of actual identity theft. Each Department with

access to such records shall provide periodic reports to the Red Flag Committee and Program Administrator. The report shall include red flags they have detected, their response, and any recommendations for changes in their Department internal policies and procedures and the City Identity Theft Prevention Program.

13) Should vendors have access to personal identifying information, Departments shall also include in contracts with vendors provisions for either the reporting of red flags to the Department or to require the vendor to prevent and mitigate the crime themselves. If the contract provides for the vendor to prevent and mitigate, the contract should also include a provision for periodic reports about the Red Flags the vendor detected and their response.

14) Each city department involved in the opening of new Records or maintenance of existing Records: Utility Customer Services, Parks and Recreation, and Information Systems shall maintain a complete, accurate, and current internal list of authorized personnel with respect to the appropriate responses in the event of a Red Flag occurring, having occurred or an actual Identity Theft; and

14) Because the City cannot predict all particular circumstances that may arise, City Personnel are requested to be diligent while not compromising customer service in the detection of other possible Red Flags.

UPDATING THE PROGRAM AND THE RED FLAGS

1) This Program will be reviewed and updated annually, or as needed, to reflect changes in risks to customers and the soundness of City Records from Identity Theft. An Assistant City Manager will be designated the Program Administrator and work with the **Red Flag Committee,** an internal City working group to consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of Records, and changes in the City's business arrangements with other entities. To do so, the Red Flag Committee and Program Administrator shall evaluate the effectiveness of the City Identity Theft Prevention Program, effectiveness of the monitoring of the practices of service providers, and will analyze significant incidents of identity theft and city response.

2) After considering these factors and recommendations from the Committee, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the Program and recommended changes to the City Council who will make a determination of whether to accept, modify or reject those changes to the Program.

3) **Note: Each City Department included in the Program shall conduct an annual Needs Assessment to ensure that their operation is current in identifying Red Flags and response protocol. See Appendix F.**

PROGRAM ADMINISTRATION AND TRAINING

1. Oversight.

The City's Program will be overseen by an Assistant City Manager and the Red Flag Committee. Committee members shall consist of the representatives of the City Manager's Office, and all other city Departments that obtain and hold personal identifying information. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

2. Staff Training and Reports.

City staff responsible for implementing the Program shall be trained under the direction of the Program Administrator, the appropriate Department Head, the Police Department and/or a combination of the above in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. **See Appendix E.** Such training will be sufficient to effectively implement the Program. All training shall be conducted annually and documented. Vendors are required to either report any red flags to the Program Administrator or respond appropriately to prevent and mitigate the crime themselves.

3. Service Provider Arrangements.

The City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1) Requiring, by contract, that service providers have such policies and procedures in place;

2) Requiring, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator; and,

3) Each Department is required to maintain an up-to-date written internal policy as it pertains to their internal security and identity theft.

Patricia Bollmann, Manager
City of Columbia, Utilities and Billing
PO Box 1676
Columbia MO 65205-1676
Phone 573-874-7458
Fax 573-874-7763
E-Mail PAB@gocolumbiamo.com

Appendix A

Finance Department Internal Identity Theft Policy
Utility Customer Services
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Ordinance

POLICY: Any person or agency requesting information regarding a customer's account must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Customers must identify themselves by the last 4 digits of their SS# before any information may be given on their account. If they can not give the last 4 digits of their SS# no information can be given.

- Telephone requests from the public for phone or social security numbers are always declined
- Persons requesting any information of a personal nature must come in person with picture ID and speak to the Manager/Supervisor.
- Faxed requests for personal information are not acceptable.
- For Realtors or prospective tenants/new homeowners it is acceptable to give information regarding high and low or average utility bills. It is not acceptable to disseminate any personal information in the notes, master file, or payment history.
- Requests for billing information from the file should only be given to the spouse, the significant other, or roommates listed in the master file or notes after they have provided the correct Social Security as verification.
- Governmental agencies; police or prosecutors requesting information should properly identify themselves. These calls should be handled by the Manager or Supervisor or the Collection staff.
- Any discussion of the details of customer's accounts outside of the office is never acceptable for any reason.
- When there is a confidential flag on an account, follow the instructions on the notes

Customer information on master file is password protected.

- Customers are not allowed in CSR Area
- Customer payment agreements are kept in the secure area.
- No paper documents may be left on desks

Janice W. Finley, Business Services Administrator
City of Columbia, Business License Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7747
Fax: 573-874-7761
E-Mail: Janice@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy
Business License Division
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code-4 of Ordinances

POLICY: Any person or agency requesting information regarding a business license customer's confidential information in their license file must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Identification of Red Flags

- Mail sent to the license applicant is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the license applicant.
- Receiving information from American DataBank Inc., the company that provides criminal background check services, concerning the inconsistency of a social security number and date of birth of a license applicant.
- The license applicant fails to provide the required personal identifying information (incomplete application).
- Receiving verbal or written information concerning an applicant submitting fraudulent documents.
- Applicant's driver's license photo is inconsistent with the person presenting the documentation.

- Owner of company listed on license application inconsistent with the Missouri Secretary of State records.

Detection of Red Flags

- Require identifying information from all license applicants.
- Verify the applicant's identity in person.
- Review documentation showing the existence of a business entity.
- Verify the identity of applicants, if they request information.

Preventing and Mitigating Identity Theft

- American Databank, Inc. monitors identifying information for inconsistencies in social security number, name, date of birth, and relays this information to the Business License Office.
- The invoices received from American Databank include only the last four digits of the applicants' social security number.
- Applicants' social security number and business gross receipts information are always deleted/blacked out on documents requested from a licensee's file.
- Social security and gross receipts information are never released unless requested by the applicant in person upon providing identification.
- Requests for confidential licensing information from City Police Department staff, Law Department staff, representatives from governmental agencies, etc., are required to obtain this information from the Business Services Administrator after providing identification.
- Inactive business license files are stored in a locked area.
- All Business License staff computers are password protected.
- Computer screens are only visible to the Business License employee when accessing licensing records.
- File cabinets that contain business license records, as well as hotel/motel and cigarette tax records, are locked at the end of each business day. The Business License area is never left unattended during office hours and access to this area is restricted to Business License staff and management.

- Always obtain copy of applicant's driver's license or other picture ID when applying for a license or permit.
- Check immigration papers to ensure validity.
- If an applicant fails to provide the requested personal identifying information, the license or permit application is denied.
- The appearance of altered or forged documents prompts further investigation.
- Double check with Missouri Secretary of State's Office to confirm members of a corporation are consistent with those listed on the application.
- Obtain criminal background check from previous state in which the applicant resided if the applicant has lived in Missouri for less than one year.
- Computer screen darkens or fades out when staff is away from their desks.
- The Business Services Administrator is the only person who can grant access to the business license system.

Ron Barrett, Comptroller
City of Columbia, Accounting Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7371
Fax: 573-874-7686
E-Mail: Ron@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy
Miscellaneous Receivables Accounting Division
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code of Ordinances

POLICY: Any person or agency requesting information regarding a miscellaneous receivables customer's confidential information in their miscellaneous receivables file must have a demonstrated right to know

PROCEDURE:

Identification of Red Flags

- Mail sent to the miscellaneous receivable customer is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the miscellaneous receivable customer.
- Receiving verbal or written information concerning a miscellaneous receivable customer submitting fraudulent documents.
- Owner of company listed on miscellaneous receivable customer inconsistent with the MO Secretary of State records.

Detection of Red Flags

- Review documentation showing the existence of a business entity.
- Verify the identity of miscellaneous receivable customer if they request information.

Preventing and Mitigating Identity Theft

- Social security numbers are never requested, used, or stored, in the miscellaneous receivable customer information system

- Requests for confidential miscellaneous receivable customer information files are provided only to city staff that are working with the miscellaneous receivable customer information as required for their department

- Customers' bank account information which is stored in the miscellaneous receivable system is maintained in a secure manner. This information is not disclosed to parties outside the miscellaneous receivable system staff.

- Inactive miscellaneous receivable customer files are stored in a locked area.

- All miscellaneous receivable customer system records are password protected.

- The appearance of altered or forged documents prompts further investigation.

- Computer screen darkens or fades out when miscellaneous receivable staff is away from their desk.

- The Accounting Assistant for miscellaneous receivables is designated as the only person who can grant access to the miscellaneous receivable system

APPENDIX B

Parks and Recreation Records Internal Identity Theft Policy
Effective October 20, 2008

PURPOSE: Establish guidelines consistent with the City of Columbia's Identity Theft Prevention Program.

POLICY: Any person or agency requesting information regarding customer's personal information must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

- All credit card and ACH banking information stored in RecTrac database is encrypted throughout the database and cannot be obtained by any user or staff.
- WebTrac (online registration) user name and passwords are set by customer. If customer forgets this information, they must know their security features they set up in order to access such information.
- E-mail and phone requests requesting customer's PIN # for online registration must confirm their mailing address, phone number and security features.
- Faxed requests are not acceptable.
- Refunds and payments are only allowed by the actual customer. There shall be no refunds or transfers of programs by individuals outside the customer's household.
- Governmental agencies; police or prosecutors requesting information must properly identify themselves. These requests should be handled by the Manager or Supervisor.
- Any discussion of the details of customer's personal information outside of the office is never acceptable for any reason.
- Scholarship assistance information shall be stored in a lockable file cabinet. Access to scholarship information shall be limited to those employees requiring access.
- The Department shall maintain an up-to-date list of those employees that are required to have access to personal records.
- Any photocopies made by Manager or Supervisor must have sensitive information (social security number, driver license number) blacked out.

APPENDIX C

Information Systems Internal Identity Theft Policy
Effective April 3, 2008

Relevant excerpts from the
City of Columbia Comprehensive Security Policy
(entire policy may be found online at
http://www.columbia.mo.gov/is/documents/security-policies.pdf)

1.3 Identification and Authentication

1.3.1 Passwords

Passwords confirm that a person is who they claim to be. As such, passwords are extremely important to the security of the City of Columbia Information System. In general, city password policy encourages a balance between complexity, rotation, and user needs. Both lenient and strict policies are generally counter productive to security. This policy instead strives to set standards that, when used together, strike an appropriate balance.

1.3.1.1 Complexity

Passwords should be greater than 8 characters, mix upper and lower case characters, and use symbols. Alternatively, passphrases can be used in the absence of passwords. For example, "AskNotForWhomTheBellTolls" is a very long password and is therefore more difficult to break. Passwords should not be easily guessed. Phone numbers, names of friends, relatives, and pets, and other personal information are generally very easy to guess.

PCI DSS 8.5.10

1.3.1.2 Rotation

Passwords should not resemble previous passwords. For example, "Password12" should not be used if "Password11" has been used before. Where possible, systems and

applications should be set to "remember" old passwords and disallow use of passwords that match or are similar to a previous password. Where possible, systems should be set to store the last 10 passwords.

PCI DSS 8.5.12

1.3.1.3 Password Responsibilities of Users

Users are responsible for choosing passwords that are reasonably complex as defined in 1.3.1.1. Users must be able to use their passwords day to day and are therefore responsible for choosing passwords that will be meaningful enough for them to remember. Users are allowed to write down their password if they are unable to remember it. If a user chooses to write down his/her password, he/she must follow these rules:

a) Their user id must not accompany the password

b) The written password must be stored in a locked location to which ONLY the user has access. The written password must never be hidden in an unlocked location.

c) The password should not be disposed of until it is no longer valid. If possible, the user should shred the password.

Users must recognize the importance of password privacy. Users must never share their password with anyone. Users must never ask each other for their passwords. Departments must make sure that business operations are such that users never need to share credentials. IT staff must never ask users for their passwords and users must understand that IT staff will never do so.

1.3.1.4 Creating and resetting passwords

Temporary passwords, whether created due to account creation or password reset, are subject to section 1.3.1.1. A temporary password created for one user should not be the same as a temporary password created for another user. Instead, temporary passwords should be random and unique.

Users should call the Helpdesk to have passwords reset for every system and application. The Helpdesk should generate a temporary password, set the password to expired, and give the user the new password. The Helpdesk should encourage the user to immediately change the password. When passwords are reset the password should never be available to the user in an electronic form. The Helpdesk shall reset the password then give the new password to the user over the phone.

When a user requests a password reset, a work order shall be immediately created before continuing. The technician resetting the passwords shall check the SecTrack application to ensure the user is allowed to use the system for which he/she is requesting the password change. If the user is not authorized to use the system for which he/she is requesting access, the technician shall inform the user that he/she needs access through the SecTrack system and he/she should speak to his/her supervisor. The success or failure of the password reset will be documented in the work order. The temporary password should not be put in the content of the work order.

Users should never be allowed to reset their password without sufficiently proving that they are who they claim to be. Systems and applications that have "Forgot Password" links should direct users to the Helpdesk instead of providing a password reset method. Helpdesk employees must take responsibility for ensuring that the person requesting a password change is who they claim to be.

If the helpdesk employee cannot verify the user's identity, the Helpdesk employee may require the user to provide "cognitive passwords," or answers to questions that only the user is likely to know. A list of questions and their corresponding answers will be maintained by the IT department, and when a user calls with a password reset request, three questions will be chosen at random. The user must be able to answer the cognitive password questions before the password is reset.

PCI DSS 8.5.2, PCI DSS 8.5.3

1.3.1.5 Password expire

Passwords shall expire every 90 days. Once a password is expired, the user shall be required to change it. All systems and applications that support password expiration should enforce this policy.

PCI DSS 8.5.9

1.3.1.6 Password Transmission and Storage

Passwords should be encrypted using hash algorithms whenever stored or transmitted. The password hash algorithm used should be evaluated in accordance with the cryptography policy.

PCI DSS 8.4

1.4.3 User privilege audits

Each system and application should have a user privilege audit at least annually. The audit should consist of two parts:

1) Department confirmation that the requested access on file in SecTrack matches the access the department wishes the user to have.

2) The access given matches the access requested in SecTrack.

Satisfies NERC CIP-003-1 R5.2

1.4.4 Account audits

Each system and application should have an account audit at least annually. The audit may be done in concert with the user privilege audit in 1.4.3. The audit should consist of two parts:

1) Enumeration of all user accounts.

2) Determination that each user account has a valid SecTrack request and that the user is still employed by the city.

NERC CIP-003-1 R5.2

1.5 Accountability and risk mitigation measures

1.5.1 Accountability

Every system and application has an accountability mechanism that differs in some way from the mechanisms of other systems and applications. Each system and applications should be evaluated and accountability mechanisms should be enabled and configured according to risk. The following are general guidelines to implementing accountability across multiple independent systems and applications.

1.5.2 Authentication logging

Systems and applications should, where possible, create log entries for authentication attempts, both successful and failed. Log entries should include user identification, date/time stamp, and the device (machine name and/or IP address) from which the attempt originated.

1.5.3 Review of authentication events

Every system and application should have its logs reviewed regularly for possible security breaches. The frequency and content of the log audits may be different for each system and should be risk based.

1.5.4 Last login information

On systems and applications where capability exists, the user should be presented with details about their last successful login. Details should include time, date, place and any other pertinent information specific to the system or application.

1.6 Administration

1.6.1 Clipping level

Accounts should not allow an infinite number of "tries" until the correct password is used. Instead systems and applications should implement a "clipping level" that locks out accounts once a certain number of failed attempts has occurred for a user id. Systems and applications that have an enforcement mechanism for this policy shall have this value set to no more than 6. If possible, the user should not be aware that their account is disabled, only that their login attempt failed. Systems and applications should lock accounts for no less than 30 minutes.

PCI DSS 8.5.13, PCI DSS 8.5.14

APPENDIX D

Columbia Police Department Notification Procedures
Effective October 24, 2008

City of Columbia Employees will routinely be exposed to situations where Identity theft is a concern. It is imperative that staff follow notification procedures to ensure that the interests of both the City of Columbia and potential victims are protected.

Employees will consistently be discussing account and customer information over the phone or in person. It is imperative that the customer identity be established prior to any account services being provided. Employees, at times, will be given conflicting or false customer information. If the information can not be clarified or substantiated by staff to a reasonable degree, the customer will be required to respond in person and show a valid form of photo I.D. Once employees are reasonably satisfied there are no identity theft concerns, services can be provided.

Employees who continue to suspect the customer of identity theft can request the assistance of the Columbia Police Department. Employees should obtain a detailed description of the suspect and be able to provide a short synopsis of the incident. Officers will respond to investigate, determine if a crime occurred and take appropriate action.

Staff will potentially discover instances of identity theft or will be notified by a customer of the crime. Employees will assist victims of identity theft with necessary information and also assist with the investigation. Employees will provide an "Identity Theft Victim Information" sheet to all potential victims. Any victims who suffer a monetary loss and are seeking potential reimbursement from the city of Columbia will be required to file a police report and assist with prosecution.

Employees will call the Columbia Police Department and an officer will respond to investigate. Staff should be prepared to provide the officer copies of original documents or any other pertinent information that can be used for the investigation. If the City of Columbia suffers a loss from the identity theft incident the officer needs to note this in the police report for potential restitution.

Employees discovering incidents of internal theft should obtain enough information for a preliminary police report. Staff should be prepared to work with investigators and gather the following information:

Case preparation guideline for embezzlement or internal theft cases

Major Crimes Division, Columbia Police Department

No one is more familiar with your bookkeeping methods than you or your accountant. Therefore, it is important that you convey that information in a manner that is easy to understand and follow. In order to assist in the investigation and prosecution of your case, it is requested that you provide documentation in the following format.

Document preparation:

When preparing your documentation, place all of the pertinent information into a three-ringed binder that is designed to hold your information secure. Original documents should be used when compiling your initial folder. Once your original binder has been completed, make three copies. Please retain one copy for your records. The original and **two** copies should be submitted to the police. Once your case has been completed, the original documents will be returned to you. **Please remember that a neat and professional product is very important.**

Overview sheet:

The overview is a "brief" narrative that provides enough details of the case that the reader can obtain a clear understanding of the incident. The following information must be included, but is not limited to:

A. Who discovered the theft and how it was uncovered.
B. Who the suspect is.
C. The dates of when the theft started and ended.
D. The theft amount.
E. How the theft was performed.
F. The names of anyone the suspect made statements to about the theft and what was said.

Narrative sheet:

Please provide a "detailed" explanation of the theft. Please include the same information from the Overview Sheet section, plus an explanation of the supporting evidence, i.e. documents, ledgers, receipts, etc. Note: This section should read like a novel, covering every aspect of the case from beginning to end. Your information may be returned for revision, if this section is not thorough. It is vital that you explain all the supporting documents in this section, so it is clear and easy to understand. All documents must be numbered. Numbering each document makes it easier for the reader to locate information, when you refer to specific figures and page numbers. You may also consider using a highlighter to aid in quick location of figures.

Itemized list

This section is composed of an itemized list of each loss, date of the loss and the supporting document page number. A total loss dollar amount should be included at the bottom of this list.

Supporting Documents:

Include all documents relating to this case, which were explained in the "Narrative" section. **If you have any questions; do not hesitate to call the detective handling your case. The investigative office can be reached at (573) 874-7423.**

Finally, employees discovering incidents of computer related crimes (hacking or similar offenses) or where customer information or employee identity theft is at risk should immediately call the Columbia Police Department to file a report and initiate an investigation. **(Emergency 911; Non-Emergency 442-6131)**

The following Identity Theft Victim Information is what responding police officers provide Identity Theft Victims:

Identity Theft Victim Information

The City of Columbia requires a Police report and cooperation in the prosecution of the person or persons responsible before any reimbursement of losses will be discussed/determined.

Place a fraud alert on your credit reports and review your credit reports:

Equifax
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Experian
1-888-EXPERIAN (397-3742)
P.O. Box 9532
Allen, TX 75013

TransUnion
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

When you report to one of these bureaus, they will report to the other two for you, and send you free reports. When you receive your reports, review them carefully. If there are any errors, report that to the credit bureaus by phone and in writing.

Close any accounts that have been tampered with or opened fraudulently, such as credit cards, bank accounts, phone and cell phone accounts, utility accounts, and internet service providers. Either use an Identity Theft Affidavit or ask the company to send you fraud dispute forms if they prefer, if there are fraudulent charges or debits.

The ID Theft Affidavit is to make sure you do not become responsible for debts incurred by the ID thief, so you must provide proof you did not create the debt. You can use the affidavit where a NEW account was opened in your name. Use it ASAP. For EXISTING accounts, your credit company will provide you with their own Dispute forms. The ID Theft Affidavit can be found at www.consumer.gov/idtheft.

If your ATM card is lost, stolen, or otherwise compromised, cancel it. Get a new card and PIN.

If your checks were stolen or misused, close that account and open a new one. Contact the three major check verification companies, and ask that retailers who use their databases not accept your checks.

TeleCheck 1-800-710-9898 or 927-0188

Certegy, Inc.	1-800-437-5120
International Check Services	1-800-631-9656

Call SCAN at 1-800-262-7771 to see if bad checks are being passed in your name.

- **File a complaint with the FTC.**

  FTC Toll-free 1-877-IDTHEFT (438-4338), www.consumer.gov/idtheft TDD 202-326-2502

  Identity Theft Clearinghouse
  Federal Trade Commission
  600 Pennsylvania Ave., NW
  Washington, DC 20580

  - Document everything: Keep originals of all correspondence and documents; send copies as necessary
  - Keep a record of everyone you talk to (names, dates, etc.)
  - Keep all your files FOREVER! If something happens at a later date, you will be glad you did
  - If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where it was filed. A list is available on the UST website at www.usdoj.gov/ust/
  - If wrongful criminal violations are attributed to your name, contact that law enforcement agency
  - Contact the Department of Motor Vehicles at www.dor.mo.gov/ and ask that your files be flagged
  - If theft of mail was involved, contact the U.S. Postal Inspection Service at www.usps.gov/websites/depart/inspect
  - If phone fraud was involved, contact the Public Utility Commission. If cell phone or long distance service was involved, contact the FCC at www.fcc.gov
  - If your social security number was involved, contact the Social Security Administration at www.socialsecurity.gov
  - If tax fraud was involved, contact the IRS at www.treas.gov/irs/ci
  - **You can find much more information about Identity Theft, with more help and guidance, at the FTC's website at www.consumer.gov/idtheft**
  - ***Information provided comes directly from the FTC's website at www.consumer.gov/idtheft***

Appendix E

Identity Theft Training Program
Effective December 1, 2008

Training Protocol

I. Introduction

a. What is Identity Theft?

II. Red Flag Legislation

a. The Federal Trade Commission's Red Flag Rule (Implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. 681.2.
b. Complying with the Red Flag Rule
c. How flexible is the Red Flag Rule?

III. The City's Identity Theft Prevention Program

a. Departments who must comply
b. Examples of Red Flags
c. What is your role and responsibility?

IV. Identity Theft

a. What is Identity Theft?
b. How does it happen?
c. How do you protect yourself from it?
d. What do you do if you're a victim?

V. How to Report

a. Your expectations
b. Notifying Law Enforcement
c. Your Assistance if investigation involved
d. What to do if a Law Enforcement response is not necessary

VI. Resources

Appendix F

Needs Assessment
Effective December 1, 2008

Conducting a Needs Assessment

Opening a New Record

Identify the steps in establishing a new record for a customer.

1) What identification is required? How do you obtain identifying information and verify identity? _____

2) Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other? _____

3) Does the Department use consumer reports in the application process? How? Establish deposit? Approve or deny services? _____

4) Does the Department have policies and procedures that define red flags for identity theft and actions for mitigation? _____

5) What happens to the hand written notes made by the Department Representative in the application process? _____

6) Is the computer screen visible to others during the application process? _____

7) Who has access to data once entered? Does the Department Representative lock computer when not at desk? _____

8) If applicant gives address, bank account, date of birth or social security number verbally to Department Representative, what precautions are taken from others hearing? _____

_____

_____

9) Once personal identification information is entered by Department Representative, where and how can it later be retrieved? _____

_____

10) What safeguards are currently built into the application process? _____

_____

_____

_____

11) What safeguards would you like to implement? _____

_____

_____

_____

12) Which employees have access to information – is it on a "need to know" basis? _____

_____

_____

_____

13) Is any customer personal information carried into the field on a laptop? _____

_____

_____

_____

Map out the steps that occur when opening a new account. Is customer identification validated? Is so, how? Trace the flow of secured information.

Customer Initial Contact

Service is established

Needs Assessment continued

Monitoring an Existing Record

Identify the possible red flags that may exist in the following procedures:

- ✓ Authenticating transactions for existing customers
- ✓ Monitoring activity/transaction of customers
- ✓ Verifying the validity of change of billing address
- ✓ Does the Department have policies and procedures that define red flags for identity theft and action for mitigation for existing records?

Does your Department use passwords or some form of security access?

_____

_____

_____

_____

Describe your process for verifying validating the following:

Check by phone_____

Credit Card Number_____

Are receipts ever printed? If so, what part of number is exposed?_____

In what manner have customers attempted to fraudulently represent themselves as someone else in a transaction in an existing account?

_____

What safeguards are currently built into monitoring existing record(s)?

_____

_____

_____

_____

What safeguards would you like to implement?

_____

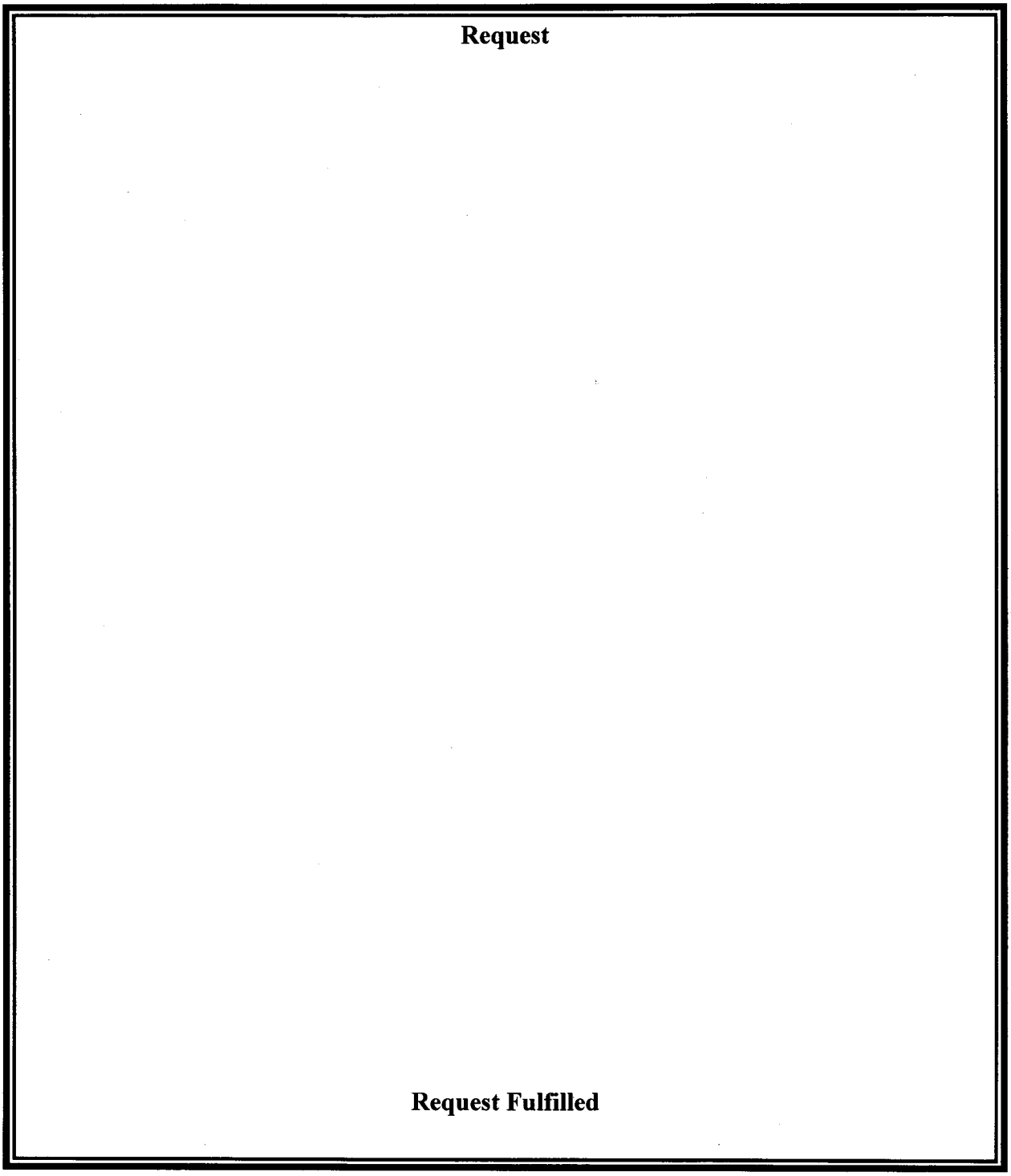
_____

_____

_____

Map out the ways customers, 3rd parties and others access existing Records.

How do you authenticate transactions for existing Records?



After you have mapped out the flow of information, identify possible areas where the protection of secured information could be improved.

EXHIBIT E

+ImageNet
Consulting

Service Level Agreement

For

City of Columbia

10-03-2022

Service Level Agreement – Software Solutions

This Service Level Agreement is made between The City of Columbia ("Client") and ImageNet Consulting, LLC ("ImageNet") on the Effective Date below.

Services

ImageNet will provide Client with certain Software Solutions services as more fully described in Appendix B to this Agreement under the terms herein.

Hardware/System Support

ImageNet shall provide support and replacement of all hardware and systems specified in Appendix B, provided that all Software is Genuine, Currently Licensed, and Vendor-Supported. Should any hardware or systems fail to meet these provisions, they will be excluded from this Service Agreement. Should 3rd Party Vendor Support Charges be required in order to resolve any issues, these will be passed on to the Client after first receiving the Client's authorization to incur them.

Coverage

Remote Helpdesk and remote technical services will be provided to the Client by ImageNet through remote means between the hours of 8:00 am – 5:00 pm Monday through Friday, except ImageNet recognized holidays. If customer is greater than 25 miles from an ImageNet office, travel costs will be charged to the client as an extension of the time of the call.

Support and Escalation

ImageNet will respond to Client's Trouble Tickets under the provisions of Appendix A, and with best effort after hours or on holidays. Trouble Tickets must be opened via our ticket entry process by submitting an email ticket to: softwaresupport@imagenetconsulting.com or by phone if internet is unavailable. Each call will be assigned a Trouble Ticket number for tracking and the client will be notified of its receipt. Our escalation process is detailed in Appendix A.

Service outside Normal Working Hours

Emergency services performed outside of the hours of 8:00 am – 5:00 pm Monday through Friday, excluding public holidays, shall be subject to provisions of Appendix B.

Service Disclaimer

Client grants ImageNet authorization to view any data within the regular routine of the repair or system improvement. Client also authorizes ImageNet to reasonably delete, change, and/or rewrite any necessary information to complete the system repair or improvement that is consistent with the standards and practices in the industry.

Excluded Services

Service rendered under this Agreement does not include:

- Post-Project on-site software technical services (see fee schedule for pricing)
- Post-Project training of administrator or end-users after project completion
- Hardware warranty or maintenance (separate agreement required)

Suitability of Existing Environment

Minimum Standards Required for Services

In order for Client's existing environment to qualify for ImageNet's Remote Technical Services, the following requirements must be met:

- All Servers, Desktop PC's and Notebooks/Laptops with Windows Operating Systems must not be past the official Microsoft extended support date and have all of the latest Microsoft Service Packs and Critical Updates installed.
- All Server and Desktop Software must be Genuine, Licensed and Vendor-Supported.
- The environment must have a currently licensed, up-to-date and Vendor-Supported Server-based Antivirus Solution protecting all Servers, Desktops, Notebooks/Laptops, and Email.
- The environment must have a currently licensed, Vendor-Supported Server-based Backup Solution that can be monitored and send notifications on job failures and successes.
- The environment must have a currently licensed, Vendor-Supported Hardware Firewall between the Internal Network and the Internet.
- All Wireless data traffic in the environment must be securely encrypted.

Chronically Failing Equipment

Experience has shown equipment belonging to the client which has initially passed Minimum Standard Requirements for system support can reveal itself to become chronically failing. This means that the equipment repeatedly breaks down and consistently causes user and business interruption even though repairs are accomplished. Should this occur, while rare, Client agrees to work constructively and positively with ImageNet to replace the equipment to ensure optimum system performance.

Term of Agreement

This Agreement is effective upon the date signed, shall remain in force for one year ("Initial Term"). Any adjustments or modifications to the terms herein must be made in writing as an amendment to this Agreement and must be signed by Client and ImageNet.

- This Agreement automatically renews for subsequent annual terms beginning on the day immediately following the end of the Initial Term unless either party gives the other thirty (30) day's prior written notice of its intent not to renew this Agreement.
- This Agreement may be terminated by either party if the other Party:
  - Breaches any material term or condition of this Agreement and fails to remedy such breach within ninety (90) days of receipt of such written notice; or
  - Terminates or suspends its business operations, unless it is succeeded by a permitted assignee under this Agreement.
- If either party terminates this Agreement, ImageNet will assist Client in the orderly termination of services, including timely transfer of the services to another designated provider. Client agrees to pay ImageNet the actual costs of rendering such assistance. Actual costs could include but are not limited to: Training, data transfer, license transfers or equipment de-installation.
- Client agrees to allow ImageNet to assign, delegate, and subcontract services to third party competent contractors approved by ImageNet.
- If there is a discrepancy between this document and the Master Service Agreement, the Master Service Agreement takes precedence.

Taxes

It is understood that any Federal, State or Local Taxes applicable shall be added to each invoice for services or materials rendered under this Agreement. Client shall pay any such taxes unless a valid exemption certificate is furnished to ImageNet for the state of use.

Limitation of Liability

In no event shall ImageNet be held liable for indirect, special, incidental or consequential damages arising under this contract, including but not limited to loss of profits or revenue, loss of use of equipment, lost data, costs of substitute equipment, or other costs.

ImageNet or its suppliers shall not be liable for any indirect, incidental, consequential, punitive, economic or property damages whatsoever (including any damages for loss of business profits, business interruption, loss of data or other pecuniary loss) arising out of this Agreement

Confidentiality

ImageNet and its agents may use Client information, as necessary to or consistent with providing the contracted services, and will use best efforts to protect against unauthorized use.

Miscellaneous

This agreement shall be governed by, construed, and enforced in accordance with the laws of the State of Missouri. Jurisdiction and venue shall exclusively lie in the County of Boone, City of Columbia. It constitutes the entire Agreement between Client and ImageNet for services listed in "Appendix B". This agreement can be modified by a signed written Addendum by both parties.

If any provision in 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 without being impaired or invalidated in any way.

ImageNet is not responsible for failure to render services due to circumstances beyond its control including, but not limited to, acts of God.

ImageNet shall comply with all federal, state, and local laws, rules, regulations, and ordinances.

Employment of Unauthorized Aliens Prohibited. ImageNet agrees to comply with Missouri State Statute Section 285.530 in that ImageNet shall not knowingly employ, hire for employment, or continue to employ an unauthorized alien to perform work within the State of Missouri. As a condition for the award of this contract, ImageNet shall, by sworn affidavit and provision of documentation, affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services. ImageNet shall also sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. ImageNet shall require each subcontractor to affirmatively state in its contract with ImageNet that the subcontractor shall not knowingly employ, hire for employment or continue to employ an unauthorized alien to perform work within the State of Missouri. ImageNet shall also require each subcontractor to provide ImageNet with a sworn affidavit under the penalty of perjury attesting to the fact that the subcontractor's employees are lawfully present in the United States.

Nature of Client's Obligations. All obligations of the Client under this Agreement, which require the expenditure of funds, are conditional upon the availability of funds budgeted and appropriated for that purpose.

No Waiver of Immunities. In no event shall the language of this Agreement constitute or be construed as a waiver or limitation for either party's rights or defenses with regard to each party's applicable sovereign, governmental, or official immunities and protections as provided by federal and state constitutions or laws.

This Agreement may be signed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document. Faxed signatures, or scanned and electronically transmitted signatures, on this Agreement or any notice delivered pursuant to this Agreement, shall be deemed to have the same legal effect as original signatures on this Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Service Agreement to be signed by their duly authorized representatives as of the date set forth below.

Fees and Payment Schedule

- Fees will be invoiced to Client on an annual basis, and will become due and payable on the first day of the renewal month. Services will be suspended if payment is not received within 10 days following the date due. Refer to Appendix B for ImageNet Services covered by the annual fee under the terms of this Agreement. Any additions to the current system at any future time will be added to the annual fee.
- It is understood that any and all Services requested by Client that fall outside of the terms of this Agreement will be considered Projects, and will be quoted and billed as separate, individual Services.

Accepted by:

Authorized Signature | City of Columbia | Date

Approved as to form:

Nancy Thompson, City Counselor/rw

Caleb Swaringim | 10-4-22

Authorized Signature | ImageNet Consulting | Date

Appendix A

Response and Resolution Times

The following table shows the targets of response and resolution times for each priority level:

Trouble	Priority	Response time (in hours) *	Resolution time (in hours) *	Escalation threshold (in hours)
Service not available (all users and functions unavailable).	1	Within 1 hour	ASAP – Best Effort	2 hours
Significant degradation of service (large number of users or business critical functions affected)	2	Within 4 hours	ASAP – Best Effort	8 hours
Limited degradation of service (limited number of users or functions affected, business process can continue).	3	Within 24 hours	ASAP – Best Effort	48 hours
Small service degradation (business process can continue, one user affected).	4	Within 48 hours	ASAP – Best Effort	96 hours

Support Tiers

The following details and describes our Support Tier levels:

Support Tier	Description
Tier 1 Support	All support incidents begin in Tier 1, where the initial trouble ticket is created, and the issue is identified and clearly documented, and basic hardware/software troubleshooting is initiated. Support provided by ImageNet
Tier 2 Support	All support incidents that cannot be resolved with Tier 1 Support are escalated to Tier 2, where more complex support on hardware/software issues can be provided by more experienced Engineers. Support provided by ImageNet & Vendor
Tier 3 Support	Support Incidents that cannot be resolved by Tier 2 Support are escalated to Tier 3, where support is provided by the most qualified and experienced Engineers who have the ability to collaborate with 3rd Party (Vendor) Support Engineers to resolve the most complex issues.

Service Request Escalation Procedure

- Support Request is Received
- Trouble Ticket is Created
- Issue is Identified and documented in Help Desk system
- Issue is qualified to determine if it can be resolved through Tier 1 Support

If issue can be resolved through Tier 1 Support:

- Level 1 Resolution - issue is worked to successful resolution
- Quality Control –Issue is verified to be resolved
- Trouble Ticket is closed, after complete problem resolution details have been updated in Help Desk system

If issue cannot be resolved through Tier 1 Support:

- Issue is escalated to Tier 2 Support
- Issue is qualified to determine if it can be resolved by Tier 2 Support

If issue can be resolved through Tier 2 Support:

- Level 2 Resolution - issue is worked to successful resolution
- Quality Control –Issue is verified to be resolved
- Trouble Ticket is closed, after complete problem resolution details have been updated in Help Desk system

If issue cannot be resolved through Tier 2 Support:

- Issue is escalated to Tier 3 Support
- Issue is qualified to determine if it can be resolved through Tier 3 Support

If issue can be resolved through Tier 3 Support:

- Level 3 Resolution - issue is worked to successful resolution
- Quality Control –Issue is verified to be resolved
- Trouble Ticket is closed, after complete problem resolution details have been updated in Help Desk system

If issue cannot be resolved through Tier 3 Support:

- Issue is escalated to Onsite Support
- Issue is qualified to determine if it can be resolved through Onsite Support

If issue can be resolved through Onsite Support:

- Onsite Resolution - issue is worked to successful resolution
- Quality Control –Issue is verified to be resolved
- Trouble Ticket is closed, after complete problem resolution details have been updated in Help Desk system

Appendix B

Service Rates

Labor	Rate
Remote Help Desk 8am-5pm M-F (30 minutes per ticket)	INCLUDED
Remote Software Access/Fix 8am-5pm M-F (30 minutes per ticket)	INCLUDED
Remote Administrator Assistance 8am-5pm M-F (30 minutes per ticket)	INCLUDED
Remote Scanner Assistance 8am-5pm M-F (30 minutes per ticket)	INCLUDED
Tier 2 Software Manufacturer Support	INCLUDED
Remote Help Desk (after 30 minutes billed in 15 min. increments) 8:00 am-5pm M-F	$165/hr.
Remote Software Access Technical/Fix (after 30 minutes billed in 15 min. increments) 8:00 am-5pm M-F	$165/hr.
Remote Administrator Assistance (after 30 minutes billed in 15 min. increments) 8:00 am-5pm M-F	$165/hr.
Remote Capture Assistance (after 30 minutes billed in 15 min. increments) 8:00 am-5pm M-F	$165/hr.
Remote Workflow/Issues (after 30 minutes billed in 15 min. increments) 8:00 am-5pm M-F	$225/hr.
Remote Migration/Issues (after 30 minutes billed in 15 min. increments) 8:00 am-5pm M-F	$225/hr.
On site Technical/Issues Labor 8:00 am – 5:00 pm (1 hour minimum)	$165/hr.
Onsite Workflow and Migration/Issues Labor 8:00 am – 5:00 pm (1 hour minimum)	$225/hr.
Onsite Labor All Other Times (1-Hr Minimum)	$ Time and a half/hr.

Any service call that causes additions, modifications, or changes to the existing system and its current functions would result in a billable charge. Example – A workflow is needed to allow for an exception to an existing process. This would go to presales engineer to scope and quote before moving forward.

Any service call that is used to resolve, maintain, or support existing functionality will not result in a billable charge. Example – A workflow stops working due to an unforeseen route or a security change, but it was working before with no changes. This would not be billable as we would be working to restore original functionality and no external changes were made.

Client would be notified of a billable event prior to it occurring.

Hardware

Servers, scanners and other hardware are covered under warranty or separate maintenance agreement.