ST. CHARLES
SINCE 1834

AGENDA ITEM EXECUTIVE SUMMARY

Title:	Recommendation to Upgrade Lawson Enterprise Resource Planning Software to Version 10 and Authorization to Contract with Ciber for Services
Presenter:	Penny Lancor

Please check appropriate box:

X	Government Operations (8/17/15)		Government Services
	Planning & Development		City Council
	Public Hearing		

Estimated Cost:	$154,884	Budgeted:	YES	X	NO	

If NO, please explain how item will be funded:

Executive Summary:

The City has been using this version of the Infor Lawson Enterprise Resource Planning software since 2011. This software runs the City's financial, payroll, procurement, accounts payable, accounts receivable, inventory, employee benefits, and Human Resources operations. As is typical with software, vendor support, eventually it is withdrawn for old versions. The City's current version will lose vendor support as of May 31, 2016. This upgrade project will bring the City's software up to the current version, assure continued support, provide an opportunity to upgrade the operating system and database server, and offer enhanced user functions.

Project costs include implementation, migration, and customization services from Ciber (with a 10% contingency) and required compiler licenses from Infor. The contingency covers unforeseen problems arising from differences discovered when migrating to a newer operating system, database, and applications. If no such difficulties are encountered, the contingency amount will remain unused.

Attachments: *(please list)*

Memo to Council (table listing costs)
Ciber Master Services Agreement
Ciber Statement of Work
Infor Net Express compiler license order form
Vendor Network Connection Agreement
City of St. Charles Confidentiality Agreement

Recommendation / Suggested Action *(briefly explain)*:

Recommendation to upgrade Lawson Enterprise Resource Planning Software to Version 10 and authorization of contract with Ciber for Services.

For office use only:	*Agenda Item Number:* 4a

Information Systems

Memo

Date: August 5, 2015

To: Alderman Dan Stellato
Chairman of the Government Operations Committee

From: Larry Gunderson, Director of Information Systems

Re: Lawson Enterprise Resource Planning software upgrade project

---

Purpose

This memorandum outlines the project to upgrade the City's Lawson ERP software from version 9.0.1 to version 10.

Background

The City has been using Infor Lawson Enterprise Resource Planning (ERP) software since 2011. This software runs the City's financial, payroll, procurement, accounts payable, accounts receivable, inventory, employee benefits, and human resources operations. Since the initial implementation the City has not upgraded the software, focusing instead on fully exploiting opportunities within existing modules. This allowed the City to realize the greatest benefit from its investment. During this time newer versions of many modules have been released. Newer versions of software offer additional functionality, bug fixes, and support for regulatory requirements.

As is typical with software, vendor support eventually is withdrawn for old versions. The City's current version will not be supported by the vendor after May 31, 2016. Vendor support allows the City to obtain updated software to accommodate regulatory changes, resolve software defects, and obtain additional functionality as it becomes available.

The Benefits of the Project

While a major driver for this upgrade is the assurance of continued vendor support, the opportunity will be taken to upgrade application infrastructure. The operating system

will be upgraded to Windows 2012 and the database server will be upgraded to SQL Server 2012. Additionally, as suggested by City auditors, database encryption will be evaluated as an enhanced security strategy.

Lawson Version 10 offers additional functionality as well. For example, the "req to check" function provides City employees with a single-screen view of related purchasing and payment data - from the initial requisition, to the purchase order, to the invoice, to the vendor payment.

The Risk of Non-action

In the event the City's software loses vendor support, a regulatory change related to payroll could leave the City vulnerable to noncompliance. For example, updates for W2 reporting requirements would be unavailable starting for tax year 2016. In addition, if security vulnerabilities were discovered within the Lawson software the City could not obtain required security patches.

Project Partner Selection Process

The Information Systems Department solicited quotes from four experienced V10 installers – Kinsey & Kinsey, RPI, TeamAbsolute, and Ciber. The core ERP team conducted conference call interviews with each vendor using a standard questionnaire. Each call lasted approximately one and a half hours and included participation by each installer's technical resources. Each vendor submitted updated quotes based on discussions from the call. Further phone calls were conducted to answer questions and clarify requirements.

The core ERP team met to prioritize vendors based on demonstrated ability to perform and overall cost. The team chose Ciber as the preferred project partner. Three references were contacted using a standard questionnaire to verify Ciber's performance on other upgrade projects. Ciber has successfully completed significantly more upgrades than other vendors. Ciber offers stability in that they are a larger organization and have at

their disposal a larger resource pool. This depth protects the City in the case of vendor staff turnover. Additionally, Ciber answered interview questions accurately and directly, and provided satisfied references. As listed in the following table, Ciber also provided the lowest proposed project cost:

Vendor	Proposed Cost	Labor Hours
Ciber	$130,440	1,064
Kinsey	$144,720	804
TeamAbsolute	$146,160	616
RPI	$154,300	844

The Project

The project consists of installing and configuring new virtual servers and migrating exiting application data, workflows, dashboards, and unique software enhancements to the new servers and applications for both a Production and Testing environment. Current integrations between Lawson and other City applications will be redefined to connect to the new servers. These integrations include financial transactions from utility billing, accounts payable checks, payroll checks and W2s to MHC, pointers to documents in Laserfiche, the online job application, and Time Entry. To facilitate use of the new version, system administration and end user training will be conducted.

Assuming City Council approval in September, we expect the project to begin by October 1, 2015. The production deployment is expected to occur in early calendar 2016.

Conclusion

Completion of the Lawson V10 upgrade project will bring the City's software up to the current version, assure continued support, provide an opportunity to upgrade the operating system and database server, and offer enhanced user functions.

City staff recommends approval of this project.

ciber

MASTER SERVICES AGREEMENT

This MASTER SERVICES AGREEMENT ("Agreement"), is made and entered into on _____, 20__ ("Effective Date") by and between Ciber, Inc., a Delaware corporation ("Ciber") and _____, a _____ corporation ("Customer") (each a "party" and together, the "parties").

RECITALS

Customer desires to contract to obtain certain information technology services and solutions to be provided by Ciber under this Agreement and Ciber desires to provide those information technology solutions and services under the terms and conditions set forth in this Agreement.

AGREEMENT

1. SERVICES

1.1 Scope of Work. Ciber will provide the services described in one or more Statements of Work signed by an authorized representative of each party (each an "SOW"). Each SOW is incorporated by reference into, and will be governed by the provisions of, this Agreement. Ciber will perform only work that is documented in an SOW. Ciber may authorize a parent, subsidiary, or affiliate of Ciber to enter into an SOW and for purposes of that SOW, such parent, subsidiary, or affiliate will be deemed "Ciber." Each SOW will describe the services to be performed ("Services"), the deliverables to be provided ("Work Products"), the schedule, the charges, and other essential information. Any inconsistency between this Agreement, an SOW, or any purchase orders or supplemental agreements, shall be decided in this order of precedence: (i) purchase orders, Confidentiality Agreement, and Vendor Network Agreement, (ii) the SOW, including all Change Orders and Acceptance/Rejection Forms (as hereinafter defined), (iii) the Agreement.

1.2 Change Orders. To modify or add work to an SOW a party must submit a written request to the other party. The recipient may accept or reject the requested modifications, or present a counter-proposal, in its sole discretion. Changes to an SOW will be effective and work commenced upon the written approval of an amendment to the SOW (a "Change Order") by an authorized representative of each party. A Change Order may include a revised price and schedule that increases Ciber's costs and time to perform the changed work. Failure to agree on any adjustment shall be a dispute under the Dispute Resolution clause of this Agreement.

1.3 Method of Performance. Ciber will determine the method, details, and means of performing the Services and providing the Work Products. Customer may require Ciber's personnel to observe Customer's safety policies and building rules when on Customer's site. Each party has the right to control its own personnel. Designation of a particular Ciber individual in an SOW does not preclude Ciber's termination or re-assignment of the individual, provided Ciber replaces the individual with a person with appropriate skills. In addition, the City has the right to request Ciber to remove an individual from the project and replace the individual with a person with appropriate skills.

1.4 Acceptance. Acceptance criteria for Services and Work Products shall be set forth in each SOW, or in such other document that the parties mutually agree in writing, including without limitation, project charters or project governance plans, which shall be incorporated into the SOW by this reference. Upon Ciber's delivery of Services or Work Products, Customer must inspect the Services and Work Products for conformance with specifications. If Ciber has not received written notice from Customer (the "Acceptance/Rejection Form") within 3 business days following completion of the Services or delivery of the Work Products, the applicable Services or Work Products will be deemed accepted by Customer. Furthermore, for other kinds of work performed by Ciber, including without limitation, staffing work for which acceptance criteria are not specified in an SOW, the applicable Services or Work Products will be deemed accepted by Customer on the date of delivery unless Ciber receives an Acceptance/Rejection Form or other written notice from Customer specifying the reason for non-acceptance within 3 business days after completion of the Services or delivery of the Work Products.

2. CUSTOMER RESPONSIBILITIES

2.1 Access and Cooperation. Customer will provide the workspaces, facilities, equipment, properly configured computers (including, hardware, software, and connectivity), and personnel described in the SOW or otherwise required by Ciber. Ciber's timely performance of the Services and provision of the Work Products are contingent on Customer promptly providing (i) all required resources, (ii) the necessary assistance and

cooperation of Customer's officers, agents, and employees, and (iii) complete, clean, and accurate information and data. If a delay is caused by Customer's failure to timely perform any obligation or deliver a necessary resource, the delivery schedule for the Services and Work Products shall be extended for the period of delay.

2.2 File Back-up. Unless otherwise specified in the SOW, Customer will maintain current comprehensive back-ups for all files, data, and programs that could be affected by the Services and implement procedures for recovering and reconstructing any files, data, and programs affected by the Services.

2.3 Health and Safety Hazards. Customer will provide Ciber with written notice of any known health and safety hazards and provide Ciber's personnel with appropriate safety procedures.

2.4 Work Rules and Conduct. Customer will provide Ciber written copies of all applicable policies and procedures, including those governing safety and security, use of equipment, sexual harassment and non-discrimination, alcohol and drug use, and integrity. Customer will report to Ciber any alleged violation of Customer's workplace conduct rules involving Ciber personnel and cooperate with Ciber in investigating the alleged violation.

2.5 Personnel Changes

i. Personnel Schedule Changes. Customer may request changes to the schedules of Ciber personnel. If Customer does not provide a written request at least 5 business days prior to the requested change, Ciber will charge Customer for the Services as scheduled.

ii. Open-ended Assignments. Customer may request termination of an open-ended assignment of Ciber personnel. If Customer does not provide a written request at least 30 days prior to the end of the assignment Ciber will charge Customer for the greater of (a) 15 days of Services that were to be performed by the affected Ciber personnel, or (b) the actual number of days of Services performed by the affected personnel after Ciber's receipt of the written request.

iii. Extension of Assignments. Ciber considers its personnel for new deployments 30 days before the expiration of their assignments. If Customer desires to extend Ciber personnel, Customer must notify Ciber at least 30 days before the scheduled expiration date to assure continued availability. Ciber will use reasonable efforts to accommodate extension requests received less than 30 days before the expiration of an assignment.

3. TERM AND TERMINATION

3.1 Term. The term of this Agreement commences on the Effective Date and continues until the date the Agreement is terminated as provided below. Termination of an SOW will not terminate the entire Agreement unless so stated in the termination notice.

3.2 Termination for Convenience. Either party may terminate this Agreement upon 60 days advance written notice. All SOWs in effect as of the Agreement's termination date shall continue until completed or terminated as provided in this Section 3.2. Unless otherwise stated in the applicable SOW, either party may terminate an SOW for time and materials Services upon 60 days advance written notice and an SOW for fixed price Services upon 90 days advance written notice. Ciber will advise Customer of the extent to which performance has been completed and deliver any work in progress. Ciber will be paid for all approved work performed and expenses incurred through the date of termination, including charges for materials ordered by Ciber that cannot be returned for a full refund. Specifically, Customer will pay (i) in full for all completed and accepted Services and Work Products, (ii) on a percentage of work performed basis, as reflected in the most recent project status report, for Services and Work Products completed by Ciber, but not accepted by Customer pursuant to Section 1.4; (iii) all of Ciber's reasonable costs to terminate and transition the work; and (iv) any cancellation fees applicable to the affected SOW as set forth in such SOW. Additionally, Customer will release all applicable retainage held by Customer and performance bonds in a form satisfactory to the bond underwriter(s).

Notwithstanding the foregoing, Customer may not terminate for convenience any SOW for outsourced Services and associated support except as set forth in the SOW. In the event Customer terminates such a SOW for convenience, Customer shall pay the cancellation fee set forth in the SOW, Ciber's charges for transition services, unabsorbed overhead costs and other general and administrative costs allocated to the terminated outsourced Services or support SOW.

3.3 Termination for Cause. Without prejudice to any other rights or remedies, either party may immediately terminate this Agreement if the other party:

i. Materially fails to perform its material obligations under this Agreement or any SOW and such failure continues for a period of 30 days after written notice;

ii. Ceases to carry on its business substantially as such business was conducted on the date of this Agreement; or

iii. Institutes or suffers a bankruptcy, reorganization, liquidation, receivership, insolvency or similar proceeding; or becomes generally unable to pay its debts as they become due.

Ciber may suspend work or terminate this Agreement or any SOW if Customer fails to pay undisputed amounts to Ciber within 15 days of Ciber's written notice specifying the undisputed amounts.

If Customer terminates this Agreement or SOW for default, Customer is obligated to pay for all undisputed Services and Work Products accepted by Customer pursuant to Section 1.4 and the unpaid portions of all disputed Services and Work Products completed by Ciber on a percentage of work performed basis, as reflected in the most recent project status report, prior to Ciber's receipt of Customer's dispute/default notice.

4. RELATIONSHIP OF THE PARTIES

Ciber is an independent contractor. Nothing in this Agreement will be construed to make Ciber or Customer partners, joint venturers, principals, agents, or employees of the other. No officer, director, employee, agent, affiliate, or contractor employed by Ciber to perform work on Customer's behalf under this Agreement will be deemed to be an employee, agent, or contractor of Customer. Neither party will have any right, power, or authority, express or implied, to bind or make representations on behalf of the other.

5. COMPENSATION

5.1 Pricing. Charges for all Services, Work Products, and expenses are set forth in each SOW. If pricing is on a T&M basis, Customer will make payments at the hourly rates in the SOW, based on a minimum per day charge of 8 hours, exclusive of sales, use, and similar taxes. Customer acknowledges and agrees that travel time to and from Customer's site is billable. Ciber will give Customer 60 days prior written notice of any change in hourly rates or prices. Ciber may impose a higher rate for Services exceeding 40 hours per week or on a weekend or holiday. Ciber does not guarantee T&M pricing estimates in any way or to any extent. If Ciber quotes a price for Services or Work Products and such price is specified without qualification in the applicable SOW, the amount quoted shall be deemed a fixed price. Unless an SOW provides for progress payments or deferral of payment after completion, Customer shall pay the full amount of the fixed price upon Ciber's completion of the specified Services or upon Customer's acceptance of the Work Products under such SOW. An SOW may provide for payment to be based on a fixed price for Services or Work Products to be rendered over a specified period of time or provide for T&M pricing not to exceed a specified amount. For fixed price onsite project work, if the travel costs are averaging over 10% of the per trip amount set forth in the SOW, Ciber will inform Customer and Ciber reserves the right to charge Customer for travel exceeding 10% of the per trip amount. Ciber will work with Customer to come up with reasonable alternatives if the travel costs exceed 10% of the budgeted amount, including performing remotely that work which is capable of being performed remotely.

5.2 Invoice and Payment. Ciber will invoice charges for third party materials purchased pursuant to an SOW upon delivery of the materials to Customer. Ciber will invoice T&M charges for Services or Work Products bi-weekly. Ciber will invoice fixed price charges for Services or Work Products in accordance with the payment schedule in the SOW. All invoices will be in Ciber's standard form and Customer agrees to receive invoices via email. Except for charges Customer disputes in good faith, all amounts are due and payable not more than 30 days from the date of acceptance for each deliverable. Customer agrees to make all payments via check. Ciber may change payment terms if, in Ciber's reasonable opinion, Customer's financial condition, previous payment record or relationship with Ciber merits such change. Customer must raise any concern or dispute in writing within 10 days from the date of the invoice or the invoice will be presumed payable. Customer's dispute of any amounts will not delay its payment of undisputed charges. If Customer defaults in payment of any charges, Ciber may immediately suspend further performance under any or all SOWs.

5.3 Taxes. Charges do not include taxes including, but not limited to, sales, use, gross receipts, and ad valorem taxes, duties or similar charges ("Taxes") imposed on the Services or Work Product (exclusive of taxes based on the property or net income of Ciber). Customer will pay or reimburse Ciber for all Taxes. If Customer is exempt from taxes, a valid tax exemption certificate or direct pay permit (collectively, "Certificate") must be provided to Ciber, Inc. upon execution of this Agreement or any applicable Taxes will be included on invoice to Customer. If Customer provides such a Certificate to Ciber, Customer agrees that Ciber is entitled to and will rely on the Certificate and that any assessment of Taxes imposed on the Services or Work Products notwithstanding the Certificate will be paid by Customer. In the event of a tax examination involving Taxes imposed on the Services or Work Products provided pursuant to this Agreement, Customer agrees to cooperate with Ciber in any such examination including responding to questions and requests for documents by the taxing authority.

5.4 Expenses. Unless expressly set forth in a SOW as included in a fixed price, Customer will reimburse Ciber for reasonable out-of-pocket expenses such as travel and living expenses. All charges exclude costs and expenses incurred for additional Services, Work Products, requirements, features, enhancements, Customer-caused delays, or expectations of Customer not explicitly stated in this Agreement or an SOW ("Additional Expenses"). Ciber will invoice Additional Expenses bi-weekly.

5.5 Interest; Collection Costs. Interest will accrue on amounts past due at the lower of eighteen percent (18%) per annum or the maximum permitted by applicable law.

6. CONFIDENTIALITY AND OWNERSHIP

6.1 Confidentiality. "Confidential Information" means any and all non-public technical or business information, including third party information, furnished or disclosed by one party to the other party that (i) the disclosing party has marked "confidential" or "proprietary"; or (ii) the disclosing party indicates is confidential or proprietary at the time of an oral disclosure and confirms is confidential or proprietary in a writing within 20 days after such oral disclosure. Each party will maintain Confidential Information it receives from the other in confidence using commercially reasonable standards and no less care than it uses with its own information, and will use and disclose such information only as contemplated by this Agreement or as authorized by the disclosing party. Each party will require its personnel to do likewise. Confidential Information does not include information that is: (a) generally available to the public other than by a breach of this Agreement; (b) rightfully received from a third party lawfully in possession of the information and not subject to a confidentiality or nonuse obligation; (c) independently developed by the receiving party or its personnel, *provided* the persons developing the information have not had access to the Confidential Information of the disclosing party; or (d) already known to the receiving party prior to its receipt from the disclosing party. Ciber agrees that "personal information" as defined in the Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq* is considered confidential information that must be protected from disclosure. If personal information is disclosed Ciber must provide immediate notice to the Customer. Ciber also agrees to comply with the provisions of the Illinois Identity Protection Act 5 ILCS 179/1 *et seq.*. Ciber shall provide a copy of its policy that sets forth how the requirements imposed on the Customer under the Illinois Identity Protection Act to protect an individual's social security number will be achieved. Ciber will provide Customer with its Data Security policy to satisfy the requirements set forth in the Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.*

6.2 Permitted Disclosures. A receiving party is permitted to disclose Confidential Information if the disclosure is (i) approved in writing by the disclosing party; (ii) necessary for the receiving party to enforce its rights under this Agreement in connection with a legal proceeding; or (iii) required by law or by the order of a court or similar judicial or administrative body, *provided that* the receiving party notifies the disclosing party of such required disclosure promptly and in writing, and cooperates with the disclosing party, at the disclosing party's reasonable request and expense, in any lawful action to contest or limit the scope of such required disclosure. In addition, Ciber shall not be required to keep confidential any ideas, concepts, know-how, or techniques developed during the course of this Agreement by Ciber personnel or jointly by Ciber and Customer personnel

6.3 Return of Confidential Information. Upon termination of this Agreement or the disclosing party's request, the receiving party will promptly return or destroy any Confidential Information of the other party.

6.4 Ownership. Unless the parties agree otherwise in writing, Work Products developed by Ciber pursuant to this Agreement belong to Customer. Customer ownership of Work Products does not extend to third party works, products, or materials or to Ciber Materials as defined below that may be included in Work Products. Customer acknowledges that Ciber is in the business of providing information technology consulting services

and has accumulated expertise in this field and agrees that Ciber will retain all right, title, and interest in and to all Ciber Materials. "Ciber Materials" means all inventions, discoveries, concepts, and ideas, including, without limitation, patents, copyrights, trademarks, trade secrets, processes, methods, formulae, techniques, tools, solutions, programs, data, and documentation, and related modifications, improvements, and knowhow, that Ciber, alone, or jointly with others, its agents or employees, conceives, makes, develops, acquires, or obtains knowledge of at any time before, after, or during the term of this Agreement without breach of Ciber's duty of confidentiality to Customer. To the extent Ciber Materials are included in any Work Products, Ciber will grant Customer a personal, perpetual, irrevocable, nonexclusive, worldwide, royaltyfree license to use, execute, reproduce, and modify such Ciber materials, but only for Customer's internal use in conjunction with the Work Products. Ciber's grant to Customer of any interest in the Services and Work Products is effective only upon Customer's payment of all fees and charges invoiced by Ciber.

6.5 Residual Rights. Either party shall be free to use Residuals (as hereinafter defined) from any Confidential Information provided by the disclosing party for any purpose, including, without limitation, providing services or creating programming or materials for customers, subject to the obligation not to disclose, publish or disseminate such Confidential Information and subject to the patent rights and statutory copyrights of the other party. **"Residuals"** shall mean that information which may be retained in intangible form in the minds of those personnel of the receiving party, without intentionally reducing such information to memory, who have had access to Confidential Information in tangible form of the disclosing party during the term of this Agreement.

7. WARRANTY AND LIMITATIONS OF LIABILITY

7.1 Warranty and Disclaimer. Ciber warrants that it will perform all Services in a professional and workmanlike manner and provide Work Products that conform in all material respects to the specifications set forth in the SOW. To receive warranty remedies, Customer must report any deficiencies to Ciber in writing within 30 calendar days from the date of Customer's acceptance of the Services or Work Products. Customer's exclusive remedy and Ciber's entire liability is to provide Services to correct the deficiencies. If Ciber is unable to correct the deficiencies, Customer is entitled to recover the fees paid to Ciber for the deficient portion of the Services or Work Products. Ciber DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR PARTICULAR PURPOSE. Ciber makes no warranties regarding Customer or third party modifications of Work Products, any portion of any deliverable developed by Customer or by any third party, including any third party software, hardware, or other third party products provided by Ciber.

7.2 Limited Liability. NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR ANY LOST DATA, LOST PROFITS, OR INCIDENTAL, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR OTHER INDIRECT DAMAGES OF ANY KIND FOR ANY REASON WHATSOEVER INCLUDING, BUT NOT LIMITED TO, DAMAGES BASED UPON, CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORY EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Except for Ciber's obligations to indemnify the Customer pursuant to Section 8.1, each party agrees that the other party's liability hereunder for damages, regardless of the form of action, will not exceed the total amount actually paid for Services and Work Products under the SOW giving rise to the damages. Notwithstanding the above, the prevailing party in any action for the collection of fees shall be entitled to reasonable attorneys' fees and court costs. The parties agree that amounts stated herein are fair under the circumstances and that the charges reflect this limitation of liability. In the event of accidental loss of or damage to tangible property, to the extent caused by the negligence of Ciber, its employees or subcontractors, the limit of liability is the maximum of insurance policy coverage.

8. INDEMNITY

8.1 General Indemnity. Ciber shall indemnify Customer and Customer's officers, directors, affiliates, subsidiaries, agents, and employees ("Customer Indemnitees") from any loss or damage arising out of a third party claim or action against Customer Indemnitees for injury to person or damage to real or tangible personal property to the extent caused by the negligent acts or omissions of Ciber's personnel while they are providing the Services to Customer under this Agreement. Customer shall indemnify and hold Ciber and Ciber's officers, directors, affiliates, subsidiaries, agents, and employees harmless from any injury to a third party or damage to real or tangible personal property of a third party to the extent caused by the negligent acts or omissions of Customer's personnel while Ciber is providing the Services to Customer under this Agreement. Neither party has a duty to indemnify or hold the other party and its officers, directors, affiliates, subsidiaries, agents, and employees harmless from or against any claim or action for injuries to person or damage to property or any

other damage or loss to the extent caused or contributed to by the act or failure to act of the other party and its officers, directors, affiliates, subsidiaries, agents, and employees.

8.2 Intellectual Property Indemnity. Ciber shall defend, and pay any damages and costs awarded in final judgment or made in settlement of, any claim or suit against Customer by a third party alleging that a Service or Work Product provided by Ciber, when used in conformity with Ciber's instructions and documentation, infringes a U.S. patent, copyright or trade secret. If any Service or Work Product is determined by a court of competent jurisdiction to be infringing, or in Ciber's opinion is likely to become the subject of a claim of infringement or violation, Ciber may, at its option, procure for Customer the right to continue using the Service or Work Product, or replace or modify the Service or Work Product so it is not infringing. If Ciber cannot secure these remedies on a reasonable basis and if Customer must discontinue use of any Service or Work Product, Ciber will refund a portion of the fees paid for the infringing Service or Work Product based on the expected life of the Service deliverable of the Work Product.

The foregoing indemnity shall not apply to any infringement claim arising from (i) a Service or Work Product that has been modified by any party other than Ciber; (ii) Customer's use of a Service or Work Product in conjunction with the products or services of parties other than Ciber where such use gives rise to the infringement claim; (iii) Customer's use of a Service or Work Product after written notice to Customer to cease such use; (iv) a Service or Work Product not used in accordance with Ciber's instructions and specifications; (v) Customer's use of other than the current release of a Service or Work Product if such claim would have been avoided by the use of the current release provided by Ciber; (vi) Customer's use of a Service or Work Product with services or products not provided by Ciber; or (vii) Ciber's compliance with any design, specification or instruction of Customer.

This Section sets forth Customer's sole and exclusive remedies for infringement or misappropriation of third party rights. Services and Work Products do not include any third party services, products or materials, whether or not supplied by Ciber.

8.3 Conditions. All indemnification under this Agreement shall be apportioned on a comparative basis taking into account the relative factors of all persons contributing to such claim or loss. An indemnifying party shall only be liable for that portion of the total indemnified claim or loss that its negligent acts or omissions bear to the negligent acts and omissions of all persons contributing to such total indemnified claim or loss.

A party's responsibility to indemnify any indemnified party is conditioned upon:

i. The indemnifying party receiving prompt written notice of any claim or action.

ii. The indemnifying party having the sole authority to defend the indemnified parties against any claim or action upon which third party indemnity is sought.

iii. The indemnified parties' cooperation with the indemnifying party's defense or settlement of the claim.

To the extent an indemnifying party's defense of the claim is materially prejudiced by an indemnified party's failure to provide prompt notice or full cooperation with indemnifying party's defense or settlement of the claim, indemnifying party shall be relieved of its indemnity obligations. The indemnifying party has no liability to indemnify or hold any indemnified party harmless for any payment by any indemnified party in settlement or compromise of a claim or action unless the indemnifying party receives written notice at least 10 business days in advance of such settlement or compromise and approves the settlement or compromise in writing before payment is made. All indemnification rights and obligations under this Agreement are subject to the terms of Section 7.2.

9. NONSOLICITATION

During the term of this Agreement and for a period of one year after its termination, neither party will directly or indirectly (i) solicit for hire or engagement any of the other party's personnel who were involved in the provision or receipt of Services or Work Products under this Agreement or (ii) hire or engage any person or entity who is or was employed or engaged by the other party and who was involved in the provision or receipt of Services or Work Products under this Agreement until 180 days following the termination of the person's or entity's employment or engagement with the other party. For purposes herein, "solicit" does not include broad-based recruiting efforts, including, without limitation, help wanted advertising and posting of

open positions on a party's internet site. If a party hires or engages, directly or indirectly, any personnel of the other party in violation of (ii) above, the hiring/engaging party will pay the other party a finder's fee equal to three times the greater of (i) gross monthly salary or (ii) monthly billing rate (assuming 168 hours per month) for such personnel.

10. DISPUTE RESOLUTION

10.1 General. Subject to each party's right to seek injunctive or equitable relief in a court of competent jurisdiction, each party agrees to resolve all disputes under this Agreement in accordance with these dispute resolution procedures.

10.2 Informal Dispute Resolution. Each party will promptly notify the other in writing of any dispute. The parties' designated representatives will meet within 10 days following the receipt of such written notice and will attempt to resolve the dispute within 5 days of the initial meeting. If the parties agree, a dispute may be mediated. The parties will select a mediator within 20 days of agreeing to mediate. All mediations shall be non-binding.

10.3 Arbitration/Other Legal Proceedings.

(a) **Arbitration.** Any claim or dispute arising out of or relating to this Agreement or the services to be provided by Ciber hereunder, other than Excluded Disputes, as defined below, shall be resolved by binding arbitration under the Commercial Rules, but not the administration, of the American Arbitration Association. To the extent the Commercial Rules conflict with this provision, this Agreement shall control any arbitration. Each party may seek preliminary or permanent rights or remedies, judicial or otherwise, to maintain the status quo until the arbitration award is rendered or the dispute is otherwise resolved. The arbitration shall be conducted in Kane County, Illinois and the laws of Illinois (except its conflict of laws provisions) shall govern the interpretation of this Agreement. Within 10 calendar days of service of a Demand for Arbitration pursuant to this Agreement, the parties shall agree upon a sole knowledgeable and impartial arbitrator. If the parties cannot agree upon a sole knowledgeable and impartial arbitrator, either party may apply to a court of competent jurisdiction for appointment of the arbitrator. If damages are to be awarded, the arbitrator shall only award equitable relief and damages in accordance with this Agreement but in no circumstances shall the arbitrator award exemplary or punitive damages.

Discovery in any arbitration shall be conducted as follows, unless otherwise agreed by the parties:

i. Discovery for each party is limited to 10 requests for production and 3 depositions, limited to 2 hours per witness.

ii. Requests for production shall be limited to documents that are directly relevant to the matters in dispute, be reasonably restricted in terms of time frame, subject matter and persons or entities to which the requests pertain and not include broad phraseology such as "all documents directly or indirectly related to." The description of custodians from whom electronic documents may be collected shall be narrowly tailored to include only those individuals whose electronic documents may reasonably be expected to contain evidence that is material to the dispute.

Each party shall pay its pro rata share of the arbitrator's fees and expenses unless the arbitrator decides otherwise. The decision of the arbitrator shall be final and binding and may not be appealed. A party may apply to any court having jurisdiction to obtain a judgment enforcing the decision of the arbitrator. The parties may cancel or terminate this Agreement in accordance with its terms and conditions without following the procedures in this Article.

(b) **Excluded Disputes.** Notwithstanding the above, Excluded Disputes shall not be subject to arbitration. As used herein, an "Excluded Dispute" means any action or proceeding with respect to this Agreement: (i) that is initiated by Ciber for collection of amounts due by Customer; or (ii) related to the allocation of ownership of Work Product or Services as between Ciber and Customer. All Excluded Disputes shall be brought exclusively in a court of competent jurisdiction located within the state of Illinois. Ciber and Customer each waive their respective rights to a jury trial in an Excluded Dispute. The laws of Illinois (except its conflict of laws provisions) shall govern with respect to such dispute. Notwithstanding subsection (a) above, if Ciber elects to initiate proceedings in court, all disputes between the parties shall be resolved in that forum.

10.4 Limit on Actions. Any dispute or other action arising out of this Agreement must be brought within two years of the date the cause of action accrued.

11. GENERAL PROVISIONS

11.1 Publicity. Ciber may reference its general business relationship with Customer for marketing purposes with the consent of the Customer.

11.2 Applicable Laws. Each party will comply with applicable foreign, federal, state, and local laws, rules, regulations, orders, ordinances, and government requirements, including without limitation, Executive Order 11246 -- Equal Employment Opportunity.

11.3 Export Controls. Neither party will knowingly export or re-export or cause to be exported or re-exported any Work Product to any country for which the U.S. government requires an export license or other government approval without first obtaining the required license or approval.

11.4 Notices. All notices must be written and will be deemed received (i) when delivered by hand, (ii) on the next business day, if delivered by a recognized overnight courier, (iii) on the third business day if mailed (by certified or registered mail, return receipt requested) or (iv) upon separately confirmed facsimile transmission to the following addresses or facsimile numbers:

CUSTOMER	**Ciber**	**Ciber Business Unit**
_____	Ciber, Inc.	_____
_____	6363 S. Fiddler's Green Circle, Suite 1400	_____
_____	Greenwood Village, Colorado 80111	_____
_____	ATTN: Law Department	ATTN: _____
Phone _____	Phone 303-220-0100	Phone _____
Fax _____	Fax 303-224-4125	Fax _____

11.5 Entire Agreement. This Agreement, the applicable Exhibits, and SOWs set forth the entire agreement of the parties relating to the Services and Work Products provided by Ciber and supersede all prior written or oral understandings, agreements, or representations by or between the parties with respect to these subjects and the parties shall not be permitted to rely on any written or oral understandings, agreements or representations made prior to execution or outside of this Agreement, any other written or oral agreements, statements or representations made outside of the four corners of this Agreement or any course of dealing, trade usage or course of performance. Any modification or waiver of this Agreement is effective only if it is in writing signed by an authorized representative of the party to be charged. Provisions of a Customer purchase order or similar document are not applicable if they conflict with or add to the terms of this Agreement.

11.6 Waiver. No delay or failure by a party in exercising any right, power, or privilege under this Agreement or any other instruments given in connection with or pursuant to this Agreement will impair any such right, power, or privilege or be construed as a waiver of or acquiescence in any default. No single or partial exercise of any right, power, or privilege will preclude the further exercise of that right, power, or privilege or the exercise of any other right, power, or privilege.

11.7 Survival. All terms and provisions of this Agreement that should by their nature survive the termination of this Agreement shall so survive.

11.8 Force Majeure. If either party is delayed or prevented from performing due to a cause beyond its reasonable control, including without limitation, strike, labor or civil unrest or dispute, embargo, blockage, work stoppage, protest, criminal acts, acts of the public enemy, acts of government in a sovereign or contractual capacity, acts of war or terrorism, or attempted acts of terrorism, or acts of God or nature, the delay will be excused during the continuance of the delay and the period of performance will be extended as reasonable after the cause of delay is removed. If a delay continues for a period of more than 30 days,

either party may terminate an affected SOW upon written notice to the other party and Customer will pay Ciber for all work performed, Work Product created and expenses incurred through the effective date of termination. Failure to make payment by Customer shall not be deemed to be a force majeure event.

11.9 Severability. If any provision of this Agreement is held invalid, void, or unenforceable to any extent, that provision will be enforced to the greatest extent permitted by law and the remainder of this Agreement and application of such provision to other persons or circumstances will not be affected. Notwithstanding the foregoing, if the invalid, void or unenforceable provision is material to the basis of the bargain of this Agreement or an SOW, or materially affects the relative economic benefits to the parties, both parties shall in good faith agree upon an equitable modification of such provision or the application thereof.

11.10 Parties in Interest. This Agreement is enforceable only by Ciber and Customer. It is not a contract or assurance regarding compensation, rights, obligations, or benefit of any kind to any other party. There are no third-party beneficiaries of this Agreement.

11.11 Assignment and Successors. Customer may not assign this Agreement without Ciber's prior written consent, except that Customer may assign the Agreement without consent to an entity controlling Customer, in common control with Customer or controlled by Customer. This Agreement benefits and will be binding upon Ciber, Customer, and their respective successors, heirs, and assigns.

11.12 Insurance. Upon request, Ciber will provide a certificate of insurance evidencing the workers' compensation, general liability, errors and omissions and automobile coverage it has in effect. Ciber, and subcontractors if applicable, shall provide insurance coverage at least as broad in not less than the following amounts unless otherwise agreed to in writing by the Customer:

Coverage Limits	
Automobile Liability	$1,000,000 Combined single limit
Commercial General Liability	$1,000,000 Per occurrence
	$2,000,000 General aggregate

All Commercial General Liability policies must include Blanket Contractual coverage and Broad Form Vendors' Liability coverage.

Workers' Compensation	$500,000 Per accident
(Employers' Liability)	$500,000 Disease limit
	$500,000 Each Disease

The parties, intending to be legally bound, have executed this Master Services Agreement on the date first set forth above.

CUSTOMER	**CIBER, INC.**
_____	_____
Signature	*Signature*
_____	_____
Print Name	*Print Name*
_____	_____
Title	*Title*
_____	_____
Date	*Date*

Lawson Version 10 Upgrade
Statement of Work

June 24, 2015

SUBMITTED BY:

ciber®

Prepared for:
Penny Lancor, Sr. Systems Analyst/Programmer

Provided by:
Jake Michael
Customer Partner
Telephone: 720.422.5863
Email: jmichael@ciber.com

Revision History

Date	Version	Description of Revision
6/24/15	*1.0*	*Initial Proposal*
7/7/2015	*2.0*	*Made updates per Customer feedback*
7/26/15	*3.0*	*Update pricing by adding Deliverables*

Protection of Confidential Information

This document contains confidential and proprietary information concerning Ciber's business, services, technology, operations and methodology. If and when the Agreement (defined in Section **Error! Reference source not found.** below) has been signed by both Ciber and Customer, "**Confidential Information**" is defined in the Agreement, and Ciber and Customer agree that all Confidential Information in this SOW is proprietary to Ciber, and is subject to, and will be handled according to, the terms and conditions in the Agreement regarding Confidential Information.

If the Agreement has not been signed by both parties at the time of receiving this SOW, by receiving and retaining this SOW, Customer agrees that, until the Agreement is signed by both parties:

(a) For purposes of this SOW, "**Confidential Information**" means all non-public technical or business information in this SOW or disclosed by Ciber to Customer in connection with this SOW;
(b) the Confidential Information is proprietary to Ciber;
(c) Customer will protect the Confidential Information using the same procedures and requirements by which it protects its own proprietary and confidential information;
(d) Customer will not disclose, in whole or in part, the Confidential Information to any person, firm, corporation, association or other entity for any reasons or purpose whatsoever in any media format;
(e) Customer will not make use of the Confidential Information for its own purposes or benefit without the prior express written consent of Ciber; and
(f) Customer will not knowingly make the Confidential Information available, in whole or in part, to current or potential competitors of Ciber or to other organizations unrelated to Customer.

If Customer is a governmental entity that must comply with requests to disclose this SOW in accordance with open/public record laws, Ciber agrees that Customer may disclose the Confidential Information to the extent necessary to comply with the applicable open/public record laws; provided that, to the extent allowed by the applicable law, Customer allows Ciber the opportunity to redact information from this SOW that constitutes trade secrets or other exceptions from the applicable open/public records laws prior to any required disclosure.

Table of Contents

1. Introduction 4

2. Scope 4

2.1. In-Scope Services 4
2.2. Out-of-Scope 5

3. Acceptance Management 5

4. Work Approach 6

4.1. Project Management 67
4.2. Technical Environment 7
4.3. Work Location 7
4.4. Work Schedule 8

5. Project Organization and Governance 8

5.1. Issues Management 8
5.2. Change Process 9
5.2.1. Change Request Process 9
5.2.2. Change Order Approvals 10
5.3. Unforeseen Conditions and Events 10
5.4. Delays and Extensions 10

6. Ciber Roles and Responsibilities 11

6.1. Ciber Roles 11

7. Customer Roles and Responsibilities 14

7.1. Customer Responsibilities 14

8. Dependencies 15

8.1. Data Protection 15
8.1.1. Ciber's Facilities; Ciber's Responsibilities 15
8.1.2. Customer's Facilities 16
8.1.3. Remote Access 16

9. Project Price 18

10. Approvals 20

Appendix A: Project Detail Breakdown 22

1. Introduction

This Statement of Work ("**SOW**"), effective on June 24, 2015, is incorporated into and is subject to the terms and conditions of the Master Services Agreement (the "**Agreement**") between Ciber, Inc. ("**Ciber**") and City of St. Charles ("**Customer**") dated _____. Any inconsistency between this SOW, implementing documents incorporated into this SOW, the Agreement, or any purchase orders or supplemental agreements, shall be decided in this order of precedence:

(a) purchase orders and supplemental agreements
(b) any approved Change Orders (defined in Section 5.2.1 below) and implementing documents to the SOW in order from the most recent to the earliest date;
(c) the SOW;
(d) the Agreement;
(e) .

Any capitalized terms that are not defined in this SOW will have the meanings given in the Agreement.

2. Scope

This section describes the Services that are In-Scope and work that is Out-of-Scope for this SOW.

2.1.In-Scope Services

Detailed description of in-scope activities can be found in Appendix A

- Installation will be remote and take place on two environments. Ciber has budgeted for two onsite trips.
- No application differences training will be provided.

- OS and Database versions to be used:

    - Windows 2012 Rx

    - SQL 2012 Rx using database encryption

- LBI will be migrated to a new install using Windows 2008 R8 and then upgraded to Windows 2012 Rx

- Self-Service applications includes EMSS and RQC (including the Mobile inbasket)

- Ming.le installed on two environments. This includes the "req to check" contextual function.

- Customizations and Processflows included within the technical development detail. This includes customized req inbasket and SQL stored procedures & SQL reporting services.

- EMSS customizations included.

- Two (2) Environment Installations

- Application upgrades

- Two (2) IPA Installations

- Two (2) LBI Installations

- One (1) LBP Repoint

- One (1) Fax Integrator installations

- Two (2) Mobile Inbasket application installations (one prod and one non-prod)

- Integration to existing BSI V10 servers for two environments

- SSL Configuration included. This includes the new ISS authentication function for EMSS outside the firewall.

- Cibergems:

- Landmark Admin IPA Workshop- Two days- Teaches users how to administer the landmark server.

2.2.Out-of-Scope

Work not specifically listed above as In-Scope is considered Out-of-Scope for this SOW. Ciber and Customer shall address alterations to the scope of this SOW through the Change Process described in Section 5.2 below.

3. Acceptance Management

Acceptance by Customer of the project's Services and Work Products means that the Services and Work Products have been completed in accordance with this SOW.

Ciber and Customer will agree upon acceptance criteria for the Services and each Work Product. Acceptance criteria must be documented as part of the Project Management Plan or Deliverable Expectation Document (DED) developed during the planning efforts of the project. Upon completion and approval by both parties, the Project Management Plan and/or DED shall be incorporated into the SOW by this reference. The parties agree to the following Acceptance Management process:

1. The Ciber Project Manager will submit an acceptance form for each completed Work Product or each completed portion, Phase or milestone of the Services and Work Products (as applicable) to the designated Customer approver.

2. Customer approver will accept or reject the Services and/or Work Product within three (3) business days from the receipt of the acceptance form from the Ciber Project Manager or communicates a reasonable timeframe in which a decision will be made.

3. If Customer approver does not accept or reject the Work Products and/or Services within three (3) business days from the receipt of the acceptance form from the Ciber Project Manager and does not communicate a reasonable timeframe in which a decision will be made, the Work Products and Services will be considered accepted.

4. If Customer rejects any Services or Work Product, the cause for rejection and all non-conformities and defects to be addressed must be documented by Customer and provided to Ciber for Ciber to correct or revise..The re-performance and/or resubmission will be evaluated by the customer, and in the case that the non-conformity or defect has not been corrected, will be resubmitted to Ciber for corrective action.

The following Customer person(s) has been designated as the approver of Work Products and Services for the project:

Name: *Penny Lancor*

Title: *Sr. Systems Analyst*

4. Work Approach

This section defines Ciber's approach to managing and delivering the Services and Work Products under this SOW.

4.1. Project Management

Ciber will plan, execute, control, and communicate the progress of the project using the Ciber Project Management Methodology (CPMM).

Ciber's PMRx® Project Portal will be used to track project progress, information, and artifacts; and to capture, track, and communicate the overall status of the project.

4.2.Technical Environment

Ciber will depend upon the technical environment described below in order to perform the Services and Work Products in this SOW.

Table 1: Technical Environment

Description: Platform, Vendor, Version	Provisioning Responsibility
Network Connectivity:	Customer will: • In accordance with the Vendor Network Connection Agreement, provide VPN or other network access to project development and test environments, and to other system environments necessary for the project, for all project members requiring access to perform their tasks. • Provide application access to applicable systems for project members. • Assign a point of contact or define a process for gaining access and resolving access issues.
Project Portal: Ciber's PMRx® Project Portal will be used to store and manage project documentation (e.g., work plans, status reports, and non-code Work Products).	Ciber will provide the PMRx® Project Portal site and manage access for all team members.

4.3.Work Location

Ciber will perform the Services from the following locations. Ciber consultants may perform certain activities remotely that are considered part of the billable Services under this SOW.

Table 2: Work Site Locations

Site Name or Location	Services Performed
Customer Location	Landmark IPA Admin Workshop, PM meetings, upgrade work
Ciber Global Solution Center(s)	Technical work (installations, migrations, etc)

Table 2: Work Site Locations

Site Name or Location	Services Performed
Ciber Office and Location	Remote consultant work will be conducted at various Ciber and consultant home offices.

4.4. Work Schedule

Ciber has defined the schedule and price based upon an average 40-hour work-week, recognizing Ciber holiday and personal leave policies for project team members, including Ciber and Customer team members. However, the project may have peak periods where the project team will be expected to work outside normal business hours. Standard Customer holidays that differ from the seven (7) holidays observed by Ciber will be scheduled work days for consultants.

-New Year's Day
-Memorial Day
-Independence Day
-Labor Day
-Thanksgiving
Christmas Day

The standard project work-week for consultants working at the Customer facility is Monday through Thursday, with four days onsite. The work-week is defined as 4-4-5— 4 nights and 4 days at Customer facility and a 5th day at a remote work location as necessary to complete the work week. Work-site arrival time on Mondays will be no later than 9:00 AM local time, with work-site departure no earlier than 3:00 PM local time on Thursday. The consultant's work-week includes up to four (4) hours per week travel time. Customer and Ciber may agree to modifications to the work week for individuals or specific work groups.

5. Project Organization and Governance

5.1. Issues Management

Throughout the Term of this SOW issues may arise requiring further information or a decision for resolution. The project team's objective is to resolve all issues at the lowest level possible. When an issue cannot be resolved at the project team level, the following escalation path will be followed. Each contact shall have the amount of time indicated in the "Response Time" column for bringing resolution to the issue, prior to the issue being escalated to the next contact level.

Table 3: Escalation Contacts

	Ciber	Customer	Response Time
First Level Contact	*<<Ciber PM>>*	Penny Lancor	Three (3) business days
Second Level Contact	*<<Ciber Client Partner>>*	Michael Drake	Three (3) business days
Third Level Contact	*<<Ciber Delivery Director>>*	Larry Gunderson	Three (3) business days

Should no resolution be reached after following this escalation path, either party may terminate this SOW as a termination for convenience subject to the Early Termination provisions below, and/or refer the dispute to the dispute resolution process defined in the Agreement, if any, and exercise any other rights and remedies available at law or in equity.

5.2.Change Process

The following Change Process will be used to manage all alterations to this SOW. Examples of alterations include but are not limited to: changes in scope, to Work Products (including accepted Work Products), to the schedule and to costs occurring for any reason, including failure of Customer to fulfill its roles and responsibilities, unforeseen events, and delays caused by Customer. Ciber will not perform services not described in this SOW until a Change Order has been approved.

5.2.1. Change Request Process

1. Either party may notify the other of requested changes by completing a "**Change Order**" ("**CO**") form which provides justification for the change and the proposed impact to the scope, schedule, and cost.

2. If Customer has initiated the CO, Ciber will respond to the CO with the impact to the scope, schedule and cost, also referred to as a CO in this process.

3. The Customer approver will approve or reject the requested Change Order within three (3) business days from the receipt of the CO form.

4. If the Customer approver does not approve or reject the requested Change Order within three (3) business days from the receipt of the CO form and does not communicate a reasonable timeframe in which a decision will be made, the requested Change Order will be considered deferred:

   a. The CO status will be logged, tracked and managed as a 'deferred' request.

   b. Services will progress without incorporating the requested change into the work plan.

   c. Where an approval or rejection decision is necessary for the Services under this SOW to progress, Ciber and Customer will use the Issues Management process above.

5. For COs outside the stated project scope, Customer will authorize budget allowance and payment, on a time and materials basis, for Ciber to perform the initial analysis of a requested change.

6. Ciber shall coordinate any changes in hardware, network, software, configuration, or Services with Customer. Customer may defer the change based on impact to business operations.

7. Ciber and Customer shall work in good faith to resolve disputes regarding the In-Scope or Out-of-Scope classification of work, using the Issues Management process above.

5.2.2. Change Order Approvals

The following persons are responsible for obtaining signature approval of Change Orders for the engagement:

Customer Name: Larry Gunderson

Ciber Name: Beth Dvoracek

Customer Role: Director of Information Systems

Ciber Role: Infor Vice President

5.3. Unforeseen Conditions and Events

If unforeseen conditions are discovered or unforeseen events occur that materially affect the original scope of work, Ciber will work with Customer to adjust the scope, cost and schedule of this SOW using the above Change Process or to terminate this SOW without penalty.

5.4. Delays and Extensions

Ciber has a limited ability to mitigate the impact of delays caused by Customer or by events outside Ciber's control. Ciber's rates, prices, and schedules do not include a contingency for the cost and schedule impacts of such delays.

Ciber will notify the Customer promptly upon discovery of any delay caused by Customer or caused by events outside Customer's or Ciber's control and Ciber will work with Customer to mitigate the cost and schedule impacts; however, Ciber will be entitled to adjust the schedule accordingly and shall inform Customer of any charges for additional work caused by such delays. Ciber will submit a Change Order for required cost and schedule adjustments. Ciber reserves the right to amend any Change Order to address the cumulative impacts of subsequent delays.

6. Ciber Roles and Responsibilities

6.1. Ciber Roles

The following main roles listed in Table 6 will be provided by Ciber. Ciber has the right to temporarily or permanently remove, re-assign and replace consultants, in its sole discretion. Ciber shall replace any assigned consultant with a consultant possessing the skills and qualifications required to perform the assigned activities. The City of St. Charles has the right to review consultant resumes and conduct phone interviews with Ciber consultants prior to assignment to the City's project.

If Customer has concerns about the skills, qualifications or suitability of any of Ciber's consultants assigned to provide Services hereunder, Customer shall promptly notify Ciber of the specific concerns. Customer and Ciber shall cooperate to correct the situation and resolve Customer's concerns promptly.

Table 4: Ciber Personnel

Role	Role Description
Project Director	The Project Director provides executive communication and issues escalation and resolution. The Project Director is ultimately responsible for Ciber's activities and deliverables. The Project Director will: • Provide support and input to CITY OF ST. CHARLES's strategic direction • Attend Project Committee and Planning Meetings • Monitors project critical success factors and the progress of work associated with the project • Resolve Ciber project issues with Project Managers • Verifies quality and completeness of all project deliverables • Enforces adherence to project methodology, processes and standards • Responsible for overall client satisfaction for the project • Assure handling of City data in a secure and confidential manner by Ciber resources while accessed on site at the City or remotely.

Table 4: Ciber Personnel

Role	Role Description
Project Manager	The Ciber Project Manager will work directly with the CITY OF ST. CHARLES Project Manager to plan, execute, and monitor the Lawson upgrade project. The Ciber Project Manager will serve as the primary agent in helping CITY OF ST. CHARLES achieve its tactical goals, including a successful implementation, a positive business relationship with Lawson, and to remain a satisfied customer of Lawson products and services. The Ciber Project Manager will also be responsible for the leadership of a team of consultants as well as assisting in the coordination of the CITY OF ST. CHARLES resources as they relate to project related tasks. The Ciber Project Manager will: • Actively work to identify and raise project issues and risks to the CITY OF ST. CHARLES Project Manager • Be responsible for managing all Ciber work efforts of the project • Coordinates and directs day-to-day activities for project team members. • Be the primary point of contact for project-related matters • Provide input and updates to project plan consisting of scope, schedule, cost, communications and risk • Maintain the overall Ciber and CITY OF ST. CHARLES project relationship • Provide guidance to the CITY OF ST. CHARLES Project Management team • Continually assess and recommend improvements to the procedures, activities, and policies that form the basis of the working relationship among CITY OF ST. CHARLES and Ciber • Provide required status reports • Provide Ciber task updates to the CITY OF ST. CHARLES Project Manager • Conduct weekly project status meetings with management team • Responsible for knowledge and DELIVERABLE transfer between on-site and off-site teams • Coordinates the Project Change Management process • Control work schedule and task assignments for technical team, including interfaces, conversions, reports • Manages effort towards meeting technical timelines • Assure handling of City data in a secure and confidential manner by Ciber resources while accessed on site at the City or remotely.

Table 4: Ciber Personnel

Role	Role Description
Technical Lead	Ciber Technical Lead provides services that address many of the IT specific needs of CITY OF ST. CHARLES. These services consist of data conversion planning and execution, interface/integration planning and development, workflow and customization design. The Senior Technical Lead will: • Assist CITY OF ST. CHARLES to establish and maintain required technical architecture and environments for development and production activities • Control work schedule and task assignments for technical team, including interfaces, conversions, reports) • Determine that technical timelines and standards are met • Prepare system test plans, technical readiness plans, and production schedules • Lead the design, implementation, and testing of the applications and security • Report on technical matters to the Project Manager(s) • Assign Technical Consultants as necessary to support technical development activities and provide project-related direction to Ciber programmers • Assess technical scope changes and impact on the overall project, and inform Project Manager(s) of those impacts • Review all technical deliverables • Oversees overall technical solution & quality • Leads key design and construction work efforts • Provides overall technical direction for the solution as defined in the SOW • Provide Operational Support • Assure handling of City data in a secure and confidential manner by Ciber resources while accessed on site at the City or remotely.

7. Customer Roles and Responsibilities

Ciber will rely upon Customer to provide the following roles and responsibilities in order for Ciber to perform the work described in this SOW. If, during the execution of this SOW, roles and responsibilities defined herein cannot be fulfilled by Customer, Ciber and Customer shall negotiate budget, schedule, or scope changes to address the deficiency.

7.1. Customer Responsibilities

Ciber will rely upon the following Customer responsibilities to perform the work described in this SOW

Table 5: Customer Responsibilities

Area	Project Responsibilities
Project Resources	Customer shall ensure that all Customer resources are available for project tasks as defined in this SOW and the Project Management Plan or other communicated schedule of activities. Customer shall ensure that assigned personnel have the skills to execute their assignments, have the authority to perform the work and make decisions, and that they fully participate in completing the effort of each task. Customer shall ensure that its personnel do not have other responsibilities outside of this project that affect their ability to perform their project assignments in a timely manner. Other Customer projects that are currently underway or may start during this project will not limit the availability of the resources, facilities, or technical infrastructure assigned for this project.
Project Information	Customer shall ensure that all information and data supplied to Ciber with respect to this project is complete, clean and accurate. Incomplete, inaccurate or erroneous information may impact the project scope, budget and/or schedule.
File Back-up	Customer will maintain current comprehensive back-ups for all files, data, and programs that could be affected by the Services and implement procedures for recovering and reconstructing any files, data, and programs affected by the Services
Policies	Customer will provide Ciber with a copy of all policies, standards and regulations applicable for these Services, and provide an initial training class for Ciber team members. Ciber will comply with such policies, standards and regulations and mutually agree with Customer on any aspects that are not applicable or are outside of Ciber's scope of work.
On-site workspace	Customer shall provide work areas, phones, network connections, and access to shared printers and conference facilities for on-site Ciber team members.

Table 5: Customer Responsibilities

Area	Project Responsibilities
Vendor Management	Customer will monitor progress of Customer vendors contributing to the project and resolves issues regarding vendor performance and/or Work Products. Customer is responsible for impacts to the project due to vendor performance issues.
Software Licenses	Customer has sole responsibility for compliance with all software license agreements, including payment of fees and providing access, developer licenses (if applicable) and user licenses to Ciber personnel in order to fulfill its responsibilities under this SOW. Customer must maintain a current support and maintenance agreement with the software vendor during the term of this SOW. Ciber does not provide any warranties for third party software or products.

8. Dependencies

Ciber will rely upon the following dependencies to perform the work described in this SOW

8.1. Data Protection

8.1.1. Ciber's Facilities; Ciber's Responsibilities

"**Ciber's Facilities"** shall mean Ciber's network environment, systems, software, equipment, premises, operations, and any other Ciber-owned and/or Ciber-managed facilities. With respect to any Services under this SOW that Ciber performs within Ciber's Facilities, and any Customer data processed, used or located within Ciber's Facilities in connection with Ciber's Services under this SOW, Ciber shall maintain, and require its personnel providing the Services to follow the following technical, procedural, and physical safeguards, which may be updated from time to time without notice to the Customer, for the protection and security of Customer's data ("**Ciber's Security Procedures**"):

a) Ciber's Employee Handbook

b) Ciber's Information Security Policy Handbook

c) Ciber's Information Security Awareness Training

d) Customer's Information Security policies and procedures as communicated to Ciber

e) Maintaining current anti-virus protection on Ciber Facilities

f) Additional security measures may be implemented depending on the type of work to be performed. All additional security measures must be documented in a written security plan and approved by both Ciber and the Customer.

With respect to Customer's Facilities (defined below) and any Services performed and any data processed, used, accessed or transmitted in or from Customer's Facilities, Customer shall have the responsibilities described below, and Ciber shall comply and require its personnel providing the Services to comply, with all Customer's Security Procedures (defined below) that are communicated to Ciber.

Ciber is entitled to rely on the established and agreed safeguards and is not responsible or liable for (a) failure of Customer to implement the required and appropriate safeguards and protections for Customer's Facilities and Customer's data, materials, and Confidential Information, (b) the acts or omissions of Customer,or any third party, including liability for any security breach or unauthorized access to data or information caused in any way by those parties; (c) any data breach, security incident, unauthorized disclosure of Confidential Information or the like that occurs even though Ciber is complying with Customer's Security Procedures and/or Ciber's Security Procedures; or (d) force majeure.

8.1.2. Customer's Facilities

"**Customer's Facilities**" shall mean Customer's network environment, systems, software, equipment, premises, operations, and any other Customer-owned and/or Customer-managed facilities. With respect to any Services under this SOW that Ciber performs in Customer's Facilities, and any Customer data processed, used, accessed, transmitted or located in or from Customer's Facilities in connection with Ciber's Services under this SOW, Customer is responsible for all physical, administrative, technical, procedural, network, and electronic data protection and other safeguards as are necessary for the protection, security, and confidentiality of any Customer Confidential Information and any data, as required by Customer's operations and applicable law for its Facilities, operations and data, including without limitation, providing appropriate notices and systems of records required under applicable laws (collectively, "**Customer's Security Procedures**"). Customer is responsible for compliance with all legal requirements with respect to Customer's Facilities. Ciber shall comply, and require its personnel providing the Services to comply, with all Customer's Security Procedures that are communicated to Ciber, while Ciber provides Services in Customer's Facilities.

8.1.3. Remote Access

If any Ciber personnel require remote access to Customer's Facilities to perform any Services under this SOW, Customer is responsible for creating a secure platform for remote access by such Ciber personnel. At a minimum this will consist of (a) the maximum allowed encryption supported by both Customer and Ciber for a VPN tunnel and (b) a terminal services environment secured and controlled by Customer with remote access granted to Ciber. This will allow for all Work Products and data to remain onsite in Customer's Facilities and in full control of Customer. Ciber personnel will not remove any Confidential

Information from Customer's Facilities via remote access. At no time will Customer grant unencrypted remote access to Ciber. Ciber will follow Customer's documented access control procedures to gain remote access to Customer's Facilities. As part of Customer's Security Procedures, Customer will provide VPN and terminal services tools, and the necessary network and environment logins to ensure that Ciber consultants will never have remote access to Customer's data except through those tools and logins. Ciber consultants will use those tools and logins for both onsite and remote access, and will not have access to any Customer data, except through those tools and logins.

9. Project Price

Except as otherwise stated in this SOW, invoice and payment terms for this project are subject to the terms and conditions of the Agreement. Ciber may suspend work on this SOW without penalty if Customer fails to pay undisputed overdue amounts to Ciber within 15 days of Ciber's written notice specifying the undisputed amounts.

Ciber has relied on the accuracy and completeness of the information provided by Customer to estimate and price the scope of this work.

All work defined within this SOW will be performed and invoiced on a Fixed Fee basis, exclusive of any applicable taxes. Applicable taxes will be invoiced in addition to these fees. Payment will be made upon completion of each deliverable, agreed to by both parties.

Consultants shall not work over 45 hours per week and no work shall be performed during off hours, weekends, or holidays unless mutually agreed to by Customer and Ciber.

Services will be rendered at the following rates. Estimated hours and amounts are indicative and may change based upon the actual work performed.

Table 6: Labor Rates

Resource	Hourly Rate	Estimated Hours	Estimated Amount
Project Manager	$200	99	$19,800
Technical Lead	$180	198	$35,640
Technical Manager	$200	77	$15,440
Upgrade Specialist	$180	66	$11,880
Global Lead	$75	306	$22,950
Global Specialist	$50	316	$15,800
Project Director	$225	2	$450
CiberGem – Landmark IPA Admin Workshop	-	Two Day Workshop	$5,000 Flat Fee
Estimated Travel		Actual Cost	$3,480
Estimated Total			**$130,440**

Deliverables	Hours		Total
Project Management Plan	20	$	4,357.00
Installed LSF System (includes all software and first data migration)	405	$	42,010.00
HCM Report Design Group 1	44	$	8,595.00
HCM Enhancements Design Group 1	143	$	27,935.00
HCM Enhancements Design Group 2	31	$	6,017.00
HCM Enhancements Development Group 1	116	$	6,268.00
HCM Enhancements Development Group 2	89	$	4,835.00
Upgrade - Initial	60	$	7,258.00
Upgrade - Integrated Test	46	$	2,507.00
Upgrade - User Acceptance Test	51	$	3,987.00
Upgrade - Cutover & Project Closure	60	$	8,190.00
Services Sub-total	**1,064**	**$**	**121,960**

*Both Test and Production environments are included in all listed in each of the deliverables above.

Custom Development Migration Design	
HCM Enhancements Design Group 2	EMSS Customization
HCM Enhancements Design Group 2	PR35.2 User Exit
HCM Enhancements Design Group 2	LP User Exit
HCM Enhancements Design Group 1	PF - Interface to GL
HCM Enhancements Design Group 1	PF - New Hire
HCM Enhancements Design Group 1	PF - Req Approval
HCM Enhancements Design Group 1	PF - AR Issue Liquor License
HCM Enhancements Design Group 1	Additional Flows
HCM Enhancements Design Group 2	.NET Applications (time keeping)
Custom Development Migration Development	
HCM Enhancements Development Group 2	EMSS Customization
HCM Enhancements Development Group 2	PR35.2 User Exit
HCM Enhancements Development Group 2	LP User Exit
HCM Enhancements Development Group 1	PF - Interface to GL
HCM Enhancements Development Group 1	PF - New Hire
HCM Enhancements Development Group 1	PF - Req Approval
HCM Enhancements Development Group 1	PF - AR Issue Liquor License
Report and Enhancement Design and Quality	
HCM Report Design Group 1	Assist with Crystal Reports & Design Studio

All travel and project related expenses incurred by Ciber will be billed to Customer utilizing Ciber's standard travel and expense guidelines at actual cost. Travel expenses cannot exceed the City of St. Charles per diem rates.

Cancellation of Scheduled Activities

With respect to any activities under this SOW that have been scheduled, Customer will provide at least ten (10) days' advance written notice to cancel any such scheduled project activity that involves any Ciber team member. If a ten-day notification is not received, Customer will be invoiced for the costs equal to any unrecoverable expenses, such as travel cancellation fees, and 50% of the billable Services for each resource involved in the activity, for up to ten days per resource of Services that would have been provided if not canceled. This applies to both future scheduled activities and activities already in progress for this SOW. This applies only to cancellation of specific activities that are part of the overall Services under this SOW, and does not apply to cancellation or termination of substantial portions of, or all remaining, Services under this SOW. The provisions of the Agreement and any specific early termination provisions of this SOW govern cancellation or termination of this SOW in whole or in part, or all remaining activities hereunder.

Early Termination

Either party may terminate this SOW for convenience upon 60 days' advance written notice.

In the event that the Services under this SOW are halted or cancelled before the Services are completed, Ciber will present an invoice to Customer for all hours worked that were not previously invoiced. Customer will pay Ciber for all Services performed, Work Product provided and expenses incurred through the date of termination, including charges for materials ordered by Ciber that cannot be returned for a full refund.

10. Approvals

IN WITNESS WHEREOF, the parties have executed this SOW on the date or dates indicated below.

BY:	BY:
Beth Dvoracek VP, Infor Practice Leader	_____ _____
Ciber, Inc.	City of St. Charles
_____	_____
Signature	Signature

Date

Date

Appendix A: Project Detail Breakdown

	Installs & Upgrade		PM & CiberGems		Project Totals	
	Hours	Amount	Hours	Amount	Hours	Amount
PLAN & MANAGEMENT						
Project Management			83	$ 16,600	83	$ 16,600
Project Planning			18	$ 3,650	18	$ 3,650
Change Management			-	$ -	-	$ -
DESIGN						
System Preparation & Support						
Software Installation	367	$ 35,190			367	$ 35,190
Business Process & Technical Analysis						
Process & Technical Analysis	-	$ -			-	$ -
Security Requirements Definition					-	$ -
Business Process Calibration (BPC)						
Brown Paper Process (As-Is)					-	$ -
Application Design (Stage 1)					-	$ -
Process To-Be Development & Workshop					-	$ -
Application Design (Stage 2)					-	$ -
Reporting Requirements					-	$ -
Project Team Education	-	$ -			-	$ -
Business Process Design & Modeling						
Pre-Pilot Activities	54	$ 6,080			54	$ 6,080
Conference Room Pilots					-	$ -
System Design	-	$ -			-	$ -
Executive Reporting Requirements					-	$ -
BUILD						
System Configuration & Setup	16	$ 3,200			16	$ 3,200
Operational Support	-	$ -			-	$ -
Technical Development	384	$ 44,940			384	$ 44,940
End User Documentation					-	$ -
End User Courseware					-	$ -
TEST						
Integrated Test	42	$ 2,100			42	$ 2,100
User Acceptance Test	38	$ 1,900			38	$ 1,900
Detailed Cutover Planning	8	$ 1,440			8	$ 1,440
ACTIVATE						
End User Training					-	$ -
Live Production Cutover	30	$ 2,540			30	$ 2,540
Post Cutover Support	24	$ 4,320			24	$ 4,320
T&M Services Total	**963**	**$ 101,710**	**101**	**$ 20,250**	**1,064**	**$ 121,960**
CiberGems (Fixed) Total				$ 5,000		$ 5,000
Expenses Total				$ 3,480		$ 3,480
Project Total	**963**	**$ 101,710**	**101**	**$ 28,730**	**1,064**	**$ 130,440**

Application Upgrade			
Task	**Hours**	**Amount**	**Notes**
DESIGN			
Technical Analysis			
Application Upgrade Strategy	-	$ -	None. Standard upgrade process will be used.
Custom Development Upgrade Analysis	-	$ -	Client responsible reviewing impact of application upgrade on all custom development, including interfaces, reports, flows, etc.
Project Team Training		$ -	None
Business Process Design & Modeling			
Upgrade Setup and Oversight	26	$ 4,680	Create Source productline, install and update upgrade software, review overall process with client.
Initial Upgraded Application Data	28	$ 1,400	Execute initial upgrade of application and environment data through completion for review prior to testing. Establishes data upgrade timing baseline as well as identification of data integrity issues to be resolved. Also provides data for modification and other technical migrations.
BUILD			
Upgrade Process Customization	-	$ -	None. Standard upgrade process will be used.
Modification Migration	384	$ 44,940	***see Technical Development Detail below***
TEST			
Integrated Test			
Integrated Test Upgrade Execution	22	$ 1,100	Re-execute application and environment upgrade for testing cycle
Integrated Test Issue Resolution	20	$ 1,000	Ciber will provide remote issue resolution support. Client to execute all testing.
User Acceptance Test			
User Test Upgrade Execution	22	$ 1,100	Re-execute application and environment upgrade for testing cycle
User Test Issue Resolution	16	$ 800	Ciber will provide remote issue resolution support. Client to execute all testing.
Detailed Cutover Planning	8	$ 1,440	Input into overall cutover and contingency plan
ACTIVATE			
Live Production Cutover	8	$ 1,440	Support for upgrade exection, cutover and reconciliation
Live Production Cutover - Remote	22	$ 1,100	Remote support for upgrade exection, cutover and reconciliation
Post Cutover Support	24	$ 4,320	Post cutover support
Totals	580	$ 63,320	

Technical Development Detail (included in the totals above)			
Custom Development Migration Design & QA	***Hours***	***Amount***	***Notes***
EMSS Customization	8	$ 1,440	EMSS Customization
PR35.2 User Exit	6	$ 1,080	User Exit in PR35.2
LP User Exit	6	$ 1,080	User Exit in LP
PF - Interface to GL	19	$ 3,420	Processflow
PF - New Hire	19	$ 3,420	Processflow
PF - Req Approval	33	$ 5,940	Processflow
PF - AR Issue Liquor License	19	$ 3,420	Processflow
Additional Flows	40	$ 7,200	Ciber to assist with additonal flows
.NET Applications (time keeping)	8	$ 1,440	Ciber to migrate .NET Time Keeping application (no development)
Custom Migration Total	***158***	***$28,440***	
Custom Development Migration Developmen	***Hours***	***Amount***	***Notes***
EMSS Customization	20	$ 1,000	EMSS Customization
PR35.2 User Exit	16	$ 800	User Exit in PR35.2
LP User Exit	16	$ 800	User Exit in LP
PF - Interface to GL	29	$ 1,450	Processflow
PF - New Hire	29	$ 1,450	Processflow
PF - Req Approval	47	$ 2,350	Processflow
PF - AR Issue Liquor License	29	$ 1,450	Processflow
Custom Migration Total	***186***	***$9,300***	
Report and Enhancement Design and Quality	***Hours***	***Amount***	***Notes***
Assist with Crystal Reports & Design Studio	40	$ 7,200	Ciber to assist with crystal reports
Enhancements Total	***40***	***$7,200***	
Technical Development Totals	***384***	***$44,940***	

Project Planning & Management			
Task	**Hours**	**Amount**	**Notes**
PLAN			
Project Management Plan			
Project Director	2	$ 450	
Project Manager	16	$ 3,200	
PROJECT MANAGEMENT			
Project Director	-	$ -	
Project Manager	83	$ 16,600	
Totals	**101**	**$ 20,250**	

Install & Environment Services

Task	Hours	Amount	Notes
DESIGN			
System Preparation & Support			
Windows LSF10 Installation	120	$ 9,000	2x LSF10 Installation. Includes BSI, Self-Service applications and current ESP & MSP. SSL configuration included.
Ming.le Installation	35	$ 2,625	2x Ming.le Workspace Installations on new SharePoint servers.
Core Landmark Installation and Federation	44	$ 3,300	2x Landmark installations. Includes WebSphere install, LDAP bind, and Federation based on 350 users. Required for Landmark products below.
Infor Process Automation Installation	4	$ 300	Includes conversion tool for initial ProcessFlow migration
EDI Professional and Comm Server Installation	-	$ -	No EDI
LBI Installation	52	$ 3,900	2x LBI installations.
Fax Integrator	8	$ 600	1x Fax Integrator Installations.
Mobile Applications	35	$ 2,625	2x Mobile applications installations
Budget & Planning Repoint	8	$ 600	2x Budget & Planning
Other consulting assistance	-	$ -	Disaster Recovery configuration, multi-webserver setup
Instllation Lead and QA	61	$ 12,240	Leadership and Issue Resolution for the above installs
BUILD			
Operational Support	-	$ -	Client will administer and maintain the system. Ciber to provide misc general support as needed throughout the project.
Ming.le Rollout	16	$ 3,200	Ciber to provide assistance with updating new portal settings. Assist setting up context
Totals	383	$ 38,390	

Price Quote

Infor Global Solutions
50 Datastream Plaza
Greenville, SC 29605

Quotation valid until: August 31, 2015

Price Quote For:
Penny Lancor, Sr. Analyst/Programmer
City of St. Charles, IL

Price Quote prepared by:
Wells Beacham
Infor Public Sector
770-625-4465
wells.beacham@infor.com

Infor Sales Rep	F.O.B Point	Currency	Payment Terms
Wells Beacham	Shipping	USD	Net 30

	Part # (if applicable)	Component System	User Restriction Quantity	User Restriction Type	Price
	BPP-MVCW-UGF	MF Net Express to MF Visual Cobol for Windows Compiler - Upgrade Fee	2	Named Users	1,424.80
	BPP-MVCW-UGF	MF Application Runtime to MF COBOL server Application Runtime - Upgrade Fee	80	Named Users	5,034.00
		Total License Fee:			**$6,458.80**
		Annual Support Fee:			**$4,941.20**
		Hosting/Subscription Fee:		-	
		Hardware Fee:		-	
		Total Amount Due(before applicable taxes)			**11,400.00**

Additional Terms

City of St. Charles, Illinois
Vendor Network Connection Agreement

This Vendor Network Connection Agreement (the "Agreement") by and between the City of St. Charles , an Illinois municipality, with principal offices in the City of St. Charles , Illinois ("City") and _____ , a _____ corporation, with principal offices at _____ ("Company"), is entered into as of the date last written below ("the Effective Date").

This Agreement consists of this signature page and the following attachments that are incorporated in this Agreement by this reference:

1. Attachment 1: Vendor Network Connection Agreement Terms and Conditions
2. Attachment 2 Network Connection Policy
3. Attachment 3: City Confidentiality Agreement

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by Illinois State law without regard to choice of law provisions.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

_____	City of St. Charles
Company	
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Name	Name
_____	_____
Date	Date

Attachment 1
VENDOR NETWORK CONNECTION AGREEMENT
TERMS AND CONDITIONS

Object: To ensure that a secure method of connectivity is provided between the City and Company and to provide guidelines for the use of network and computing resources associated with the Network Connection as defined below.

Definition: "Network Connection" means one of the City connectivity options listed in Section B of the Network Connection Policy.

1. Right to Use Network Connection. Company may only use the Network Connection for business purposes as defined in an approved scope of work, agreement or contract with the City.

2. Network Security

   a. Company will allow only Company employees approved in advance by City ("Authorized Company Employees") to access the Network Connection and any City -Owned computing resources. Company shall be solely responsible for ensuring that Authorized Company Employees will not pose a security risk, and upon the City's request, Company will provide the City with any information reasonably necessary to evaluate security issues relating to any Authorized Company Employee.
   b. Authorized Company Employees will only be provided credentials that are unique to each user (i.e. no "generic" usernames and passwords) to access City -Owned computing resources. Usernames and passwords cannot be shared with anyone.
   c. Company will promptly notify the City whenever any Authorized Company Employee leaves Company's employ or no longer requires access to the Network Connection and City -Owned computing resources.
   d. Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the Network Connection (and Company's use of City -Owned computer resources) is secure and is used only for authorized purposes, and (b) such party's business records and data are protected against improper access, use, loss alteration or destruction.

3. Notifications. Company shall notify City in writing promptly upon a change in the user base for the work performed over the Network Connection or whenever in Company's opinion a change in the connection and/or functional requirements of the Network Connection is necessary.

4. Payment of Costs. Each party will be responsible for all costs incurred by that party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

5. Confidentiality. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the other's business records, technology and products that is confidential and of substantial value to that party, which value would be impaired if such information were disclosed to third parties ("Confidential Information"). Should such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure. If Confidential Information is disclosed by the Company and is considered "personal information" as defined in the Illinois Personal Information Protection Act, 815 ILCS 530/1 *et seq.* Company must provide immediate notice to the City. Each party agrees that it will not use in any way for its own account, except as provided herein, nor disclose to any third party, any such Confidential Information revealed to it by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information. Upon request by the receiving party, the disclosing party shall advise whether or not it considers any particular information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information. The receiving party's obligation of confidentiality shall not apply to information that: (a) is already known to the receiving party or is publicly available at the time of disclosure; (b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or (c) becomes publicly available after disclosure through no fault of the receiving party.

6. Term, Termination and Survival. This Agreement will remain in effect until terminated by either party. Either party may terminate this agreement for convenience by providing not less than thirty (30) days prior written notice, which notice will specify the effective date of termination. Either party may also terminate this Agreement immediately upon the other party's breach of this Agreement. All terms and provisions of this Agreement that should by their nature survive the termination of this Agreement shall so survive.

7. Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

8. Waiver. The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

9. Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.

10. Force Majeure. Neither party will be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

Attachment2
NETWORK CONNECTION POLICY

Purpose: To ensure a secure method of network connectivity between City and its vendors and to provide a formalized method for the request, approval and tracking of such connections.

Scope: External data network connections to City can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the City network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts.

Definitions: A "Network Connection" is defined as one of the connectivity options listed in Section B. below. "Vendor" is defined as the City's Contractors, Suppliers and the like.

A. Vendor Network Connection Requests and Approvals

All vendor network connection requests must have the signature of the City Administrator, or his/her designee, for approval. Also, all vendors requesting a Network Connection must complete and sign a City Confidentiality Agreement.

B. Connectivity Options
The following connectivity options are the standard methods of providing a Vendor Network Connection. Anything that deviates from these standard methods must have written authorization from the City.

1) Private Leased line – Dedicated, Private Leased lines for vendors will be terminated on the Partner's network. These circuits can be delivered as T1 or Ethernet.

2) Encrypted Tunnel – Encrypted tunnels must be terminated on the vendor's Network, whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel in the City's DMZ, in which case the normal City perimeter security measures will control access to Internal devices.

3) Remote Access – Remote Access through a third party or directly via Internet remote control shall be determined by the City.

C. Protection of Information and Resources
The Company shall be held legally responsible for misuse of its access and use of the City's network and computing resources. The Company shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information. This includes the requirement that a City-approved

virus protection software program is installed. This program must be operational and be using the latest virus detecting upgrades for computers used for this purpose.

The Company will not:

a. Attempt to disguise their identity, or the identity of their account.
b. Attempt to impersonate other persons or organizations.
c. Appropriate the City's name, or its network names.
d. Attempt to monitor other users' data communications unless specifically authorized.
e. Infringe upon the privacy of others' computer files.
f. Read, copy, change, or delete another user's computer files or software without the prior express permission of the owner.
g. Engage in actions that interfere with the use by others of any computers and networks, interfere with the supervisory or accounting functions of the systems, or are likely to have such effects.
h. Attempt to bypass computer or network security mechanisms without the prior express permission of the City's Information Systems Department. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent of such an attempt

D. Audit and Review of Vendor Network Connections

All aspects of Vendor Network Connections - up to, but not including the Company's firewall, may be monitored by the City's Information Systems Department.

E. City Information Systems Department Responsibilities

The City's Information Systems Department is responsible for the installation and configuration of a specific Vendor Network Connection and will ensure that all possible measures have been taken to protect the integrity and privacy of City confidential information. At no time will the City rely on access/authorization control mechanisms at the Company's site to protect or prohibit access to City confidential information.

The City's Information Systems Department has the responsibility for maintaining related policies and standards and will be the sole judge determining if the Company has complied with the Vendor Network Connection policy. The Information Systems Department is also responsible for approval of firewall design, configuration and engineering required for support of Vendor Network Connections.

Attachment 3

CONFIDENTIALITY AGREEMENT

This Agreement is made between _____ ("Company"[1]), with offices located at _____, and the City of St. Charles ("City"), with offices located at 2 E. Main Street, St. Charles, Illinois 60174 (each a "Party" hereto).

RECITALS

WHEREAS, the City and Company may provide each other certain proprietary, confidential, non-public, or trade secret information.

WHEREAS, the Parties wish to set out the terms under which each Party is willing to disclose such information to the other Party and upon which the Parties are willing and obliged to keep such information confidential.

NOW THEREFORE, the Parties agree as set out below:

1.0 **DEFINITIONS.** In addition to those words defined above, the following words shall have the meanings set forth below.

1.1 **CONFIDENTIAL INFORMATION** means all documents or information disclosed or made available by the City and the Company in connection to:

1.1.1 opinions expressed or policies or actions that are formulated, including, but not limited to, preliminary drafts, notes, recommendations, memoranda and other records, as well as technical information related to the security systems of the City, including physical and logical access controls and computer networks, or the security of other records which are exempt from disclosure under the Illinois Freedom of Information Act, in addition to other state and Federal exemptions, as may be applicable;

1.1.2 all Personal Identifying Information (PII). Personal identifying information is staff, contractor, or customer information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual;

1.1.3 medical or health records, and personnel information;

1.1.4 documents, including:

(a) any text, letter, memorandum, sound recording, videotape, film, photograph, chart, graph, map, survey, diagram, model, sketch, book of account and

[1] Whenever the word "Company" is used herein, it shall be deemed to be defined to include all current and former employees, agents and representatives of the Company.

information recorded or stored by means of any device pertaining to the City and/or any of its information technology or other systems and marked "Confidential" or "Proprietary.";

(b) technical data, research, products, financial information, plans or strategies, forecasts or forecast assumptions, business practices, operations, procedures or services related to the City and/or any of its information technology or other systems and marked "Confidential" or "Proprietary.";

1.2 SUBSIDIARY OF A PARTY means any corporation or individual that is controlled by the Party, and refers to a direct or indirect subsidiary of the Party.

2.0 AGREEMENT

2.1 Each party agrees:

(a) to use the same means it uses to protect its own confidential information to maintain the secrecy and confidentiality of the other Party's Confidential Information,

(b) except as provided in Sections 2.1(d), 2.2 and 2.4, not to disclose any Confidential Information to a third party without the prior written consent of the Disclosing Party,

(c) not to use any Confidential Information for any purposes other than providing bids or quotes or fulfillment of a Contract,

(d) only to disclose the Confidential Information to its directors, officers, employees, agents and advisers (collectively called "Representatives") who have a need to know the information for the creation of bids or quotes or for the fulfillment of a Contract (it being understood that the Receiving Party shall inform such Representatives of the confidential nature of that information and the obligation of confidentiality undertaken by the Receiving Party hereunder, and shall direct such Representatives to treat that information confidentially in accordance with the terms of this Agreement),

(e) to take reasonable steps to prevent its Representatives from acting in a manner inconsistent with the terms of this Agreement, and

(g) Maintain the confidentiality of computer system passwords. The following actions by either Party will be considered a violation and breach of this Agreement:

- Disclosing a password to another person.
- Using another person's ID or password, with or without that person's knowledge or consent.
- Using access to shared computer facilities for other than services hereunder.

Any ID that is assigned will be provided with a level of access that is adequate to perform services hereunder. Attempts by either Party to access information that are outside these bounds will be considered a violation and breach of this Agreement.

(h) to establish information security standards requiring that reasonable measures be implemented that are designed to:

1) Ensure the security and confidentiality of any of City's confidential information in your possession or control;

2) Protect against any anticipated threat or hazards to the security or integrity of this information;

3) Encrypt any PII data stores that reside on portable media or devices, such as laptops, thumb drives, external hard drives or CDs;

4) Protect against unauthorized access to or use of this information that could result in substantial harm or inconvenience to any staff, contractor, or customer of the City; and

5) Ensure the proper disposal of this information.

2.2 This Agreement does not impose any obligations on the Company with respect to its own Confidential Information. In addition, the obligations of confidentiality set out above do not apply to information that:

(a) at the date of disclosure said information (in the same form in which the disclosure is made) has been published or has otherwise entered the public domain without a breach of this Agreement, or thereafter becomes generally available to the public without breach of this Agreement. If any of the information described as Confidential in Paragraph 1.1 above is alleged to have become public, before disclosing such information to any other person the Party so claiming will notify the City and obtain written confirmation that it is likewise the City's understanding that such Confidential Information has entered the public domain;

(b) is independently developed or obtained by the receiving Party without breach of this Agreement. Prior to use of such information, the Company shall notify the City in writing if it intends to use or in any way reference or discuss Confidential Information which it believes has been independently developed or obtained by either of them without breach of this Agreement.

2.3 It is not a breach of this Agreement to:

(a) disclose Confidential Information required to be disclosed by applicable law, regulation or court order in which event the receiving Party shall (unless affirmatively prohibited by such applicable law, regulation or court order) promptly notify the City in writing of the requirements for such disclosure and cooperate through all reasonable and legal means, at the City's expense, in any attempts by the disclosing Party to prevent or otherwise restrict disclosure of the Confidential Information.

(b) Disclose any ideas, concepts, know-how, or techniques developed during the course of the Agreement by Company personnel or jointly by Customer and City personnel.

2.4 The Parties agree that certain Confidential Information may be subject to attorney-client work product or other privileges and that no disclosure hereunder is intended to waive any privileges applicable to any statement, document, communication, or other information disclosed pursuant to this Agreement. The receiving Party shall treat such Confidential Information accordingly.

3.0 NO WARRANTY

3.1 The Parties make no representations or warranties about the adequacy, accuracy, or suitability of the Confidential Information for any purpose. The receiving Party is responsible for making its own evaluation of such Confidential Information.

3.2 Each Party acknowledges that notwithstanding the execution of this Agreement, the City maintains the sole and absolute discretion to determine what, if any, information it will release to the Company or which it will allow the Company to use.

4.0 REMEDIES

4.1 The Parties acknowledges that a breach of this Agreement may cause serious and irreparable harm that may be difficult to ascertain. In the event of breach of this Agreement by either Party , the Party shall be entitled to obtain immediate injunctive relief in addition to any other rights or remedies it may have without proof of any actual or special damages and without the requirement to post bond or other surety in connection with any such injunctive relief. The prevailing Party shall be entitled to all attorneys' fees and costs incurred in such action or actions

5.0 RETURN OF INFORMATION

At any time the City may request the return or the destruction, of all tangible Confidential Information previously delivered to the Company. Upon receipt of such request, all such Confidential Information, including without limitation any copies, summaries or compilations of such information, still in the Company's possession or under its control shall be promptly returned or destroyed, as requested.

6.0 MISCELLANEOUS

6.1 The nondisclosure provisions of this Agreement shall survive the termination of this Agreement, and the Company's duty to hold Confidential Information in confidence shall remain in effect until the City notifies it in writing that such information no longer qualifies as Confidential Information or sends the Company written notice releasing it from this Agreement, whichever occurs first.

6.2 This Agreement may be modified only in a document signed by the Parties.

6.3 No party shall assign, transfer, convey, or otherwise dispose of its rights, title, or interest in or to this Agreement or any part thereof without the previous written consent of the other Parties.

6.4 This Agreement is governed by the laws of the State of Illinois without giving effect to its conflict of laws provisions and is treated in all respects as an Illinois contract. Venue for any action arising out of the terms or conditions of this Agreement shall be proper only in the Circuit Court for the Sixteenth Judicial Circuit, Kane County, Illinois.

6.5 If any provision of this Agreement is held to be invalid, illegal, or unenforceable, all other provisions will, nevertheless, continue in full force and effect.

6.6 This Agreement inures to the benefit of the Parties and is binding upon their respective successors and assigns.

6.7 The Parties agree that this Agreement:

(a) is the complete and comprehensive statement between the Parties about the protection of the secrecy or confidentiality of the Confidential Information; and

(b) supersedes all discussions and other communications, whether written or verbal, between the Parties related to the protection of the secrecy or confidentiality of the Confidential Information.

6.8 The provisions of this Agreement shall survive the completion of the Purpose as defined herein.

6.9 This effective date of this Agreement ("Effective Date") shall be the last date on which either of the Parties hereto execute this Agreement.

IN WITNESS WHEREOF, the Parties have signed this Agreement on the dates indicated below and acknowledge that they have read and understand this Agreement and voluntarily accept the duties and obligations set forth herein.

CITY OF ST. CHARLES	**COMPANY**
By:_____ (Signature)	By:_____ (Signature)
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

PRESENTER

By:_____
(Signature)

Name: _____

Title:_____

Date:_____