R 46-16

City of Columbia

701 East Broadway, Columbia, Missouri 65201

Department Source: Finance
To: City Council
From: City Manager & Staff
Council Meeting Date: April 18, 2016
Re: Paymentus Master Services Agreement

Executive Summary

A resolution authorizing the City Manager to enter into a contract with Paymentus, who acquired Tele-Works Incorporated (TWI), for the implementation of a hosted multi-channel billing, payment and automation solution for utility billing and incorporation of a convenience fee.

Discussion

At Council's request, the Department of Finance has worked with the current on-line and telephone billing payment processor to upgrade the payment processing platform and integrate with the City's new utility billing system. This contract will also lower the convenience fee charged to residential customers from $4.60 per $1,000 transaction to $3.55 per $750 transaction for all utility payments made via the internet or telephone.

Fiscal Impact

Short-Term Impact: Continued savings of bank processing fees and software maintenance cost.
Long-Term Impact: Annual savings of approx. $350,000 to $400,000 in bank processing fees and software maintenance cost.

Vision & Strategic Plan Impact

Vision Impacts:
Primary Impact: Governence & Decision Making, Secondary Impact: Secondary, Tertiary Impact: Tertiary

Strategic Plan Impacts:
Primary Impact: Social Equity, Secondary Impact: Secondary, Tertiary Impact: Tertiary

Comprehensive Plan Impacts:
Primary Impact: Primary, Secondary Impact: Secondary, Tertiary Impact: Tertiary

Legislative History

Date	Action
02/20/2012	B-39 was introduced to amend language in the ordinance to allow the finance director to offer a discount to large utility customers. Council approved an amendment to the proposed bill to remove the discount language and change it to a service fee and tabled the bill until March 5, 2012.
03/05/2012	B-39-12A was passed authorizing the Finance Director to move forward with the implementation of the fee.
10/05/2012	R173-12 was passed by Council, which authorized the City Manager to enter into a contract with Tele-Works, Inc. (TWI) for their Summation 360 Solution Suite which incorporated a $4.60 convenience fee for those customers who pay on-line or via the telephone.
09/03/2013	R170-13 was passed by Council, which authorized an Amendment to the Tele-Works, Incorporated agreement to allow Automated Clearing House (ACH) processing for electronic checks.

Suggested Council Action

Approval of the Resolution authorizing the City Manager to enter into the contract with Paymentus.

Introduced by ____________________________ Council Bill No. R 46-16

A RESOLUTION

authorizing a master services agreement with Paymentus Corporation for implementation of a multi-channel billing, payment and automation solution for utility billing; authorizing an agreement with Paymentech, LLC, on behalf of JPMorgan Chase Bank, N.A., for payment processing services.

BE IT RESOLVED BY THE COUNCIL OF THE CITY OF COLUMBIA, MISSOURI, AS FOLLOWS:

SECTION 1. The City Manager is hereby authorized to execute an agreement with Paymentus Corporation for implementation of a multi-channel billing, payment and automation solution for utility billing. The form and content of the agreement shall be substantially as set forth in "Exhibit A" attached hereto and made a part hereof.

SECTION 2. The City Manager is hereby authorized to execute an agreement with Paymentech, LLC, on behalf of JPMorgan Chase Bank, N.A., for payment processing services. The form and content of the agreement shall be substantially as set forth in "Exhibit B" attached hereto and made a part hereof.

ADOPTED this ______ day of ____________________________, 2016.

ATTEST:

________________________________ ________________________________
City Clerk Mayor and Presiding Officer

APPROVED AS TO FORM:

____
City Counselor

Exhibit A

Paymentus

MASTER SERVICES AGREEMENT

Client:	City of Columbia MO
Client Address:	701 E. Broadway Columbia, MO. 65205
Contact for Notices to Client:	Cale Turner
Estimated Yearly Bills / Invoices:	$625,000

This Master Services Agreement ("Agreement") by and between the City of Columbia, Missouri, a Missouri municipality, and Paymentus Corporation, a corporation organized in the State of Delaware with authority to transact business within the State of Missouri, is made and entered into as the date of the last signatory noted below (hereafter "Effective Date").Client and Paymentus are each individually referred herein as a "Party" and collectively as the "Parties."

WHEREAS, Client desires to allow Client's utility customers to pay their utility bills via credit cards, debit cards, and electronic checks; and

WHEREAS, Paymentus represents that it's software and services shall provide the functionality and security required by this Agreement and applicable laws to allow for the secure payment of utility bills via credit cards, debit cards, and electronic checks; and

WHEREAS, Client desires to receive certain services under the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants hereinafter set forth, for good and sufficient consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties, intending to be legally bound, hereby covenant and agree as follows.

GENERAL TERMS AND CONDITIONS

1 Definitions:

For the purposes of this Agreement, the following terms and words shall have the meaning ascribed to them, unless the context clearly indicates otherwise.

1.1 "**Agreement**" or "**Contract**" shall refer to this Agreement, as amended from time to time, which shall constitute an authorization for the term of this Agreement for Paymentus to be the provider of services, stated herein, to the Client.

1.2 "**User**" shall mean the Client's utility customers.

1.3 "**Effective Date**" shall be the last date upon which the Parties signed this Agreement. The Agreement will not be effective against any Party until the said date.

1.4 "**Payment**" shall mean payments made by Users for utility services.

1.5 **"Payment Amount"** shall mean the bill amount User wants to pay to the Client for utility services.

1.6 "**Services**" shall include the performance of the Services outlined in Section 2 of this Agreement.

1.7 **"Paymentus Authorized Processor"** shall mean a Paymentus authorized merchant account provider and payment processing gateway.

1.8 "**Reversed or Charged-back Transactions**" shall mean cancelled transactions due to User error, or a User's challenge to Payment authenticity.

1.9 "**Average Bill Amount**" shall mean the total amount of residential Payments collected through Paymentus system in a given month divided by the number of the residential Payments for the same month.

2 Description of Services to be Performed

2.1 Scope of Services

a) Paymentus shall provide Users the opportunity to make Payments by Visa, MasterCard, Discover, and other payment card brands mutually agreed by the Parties in writing and E-check. Payments may be made by Interactive Telephone Voice Response System ("IVR") or secure Internet interface provided at the Paymentus Corporation's web site or other websites part of Paymentus' Instant Payment Network ("WebSites"), collectively referred to as the ("System").

b) Paymentus shall provide Users a secure electronic way to register their account(s); manage paper or electronic bill settings; maintain e-mail address and password; view history for billing statements for at least twelve months, consumption and payments; real-time account access and payment posting.

c) Paymentus shall provide to Client software and services with the following required functionality:

   a. Through the use of Paymentus software and services Client shall have the ability to schedule, in advance, and send outbound notifications to Client's utility customers to deliver messages via phone, text or e-mail. Client shall be responsible for the message content.

   b. Client shall have access to reports showing call out attempts, including final disposition of each call that was placed.

c. The Paymentus software and services shall allow Client's utility customers the option to securely pay directly from the outbound call.

d. The Paymentus software and services shall give User the ability to opt-in or opt-out of receiving messages.

2.2 Professionalism

Paymentus shall perform, in a professional manner, all Services required to be performed under this Agreement. Paymentus shall also maintain compliance with all Payment Card Industry (PCI) Standards, regulations set by the Visa, Mastercard, Discover, and other payment card brands mutually agreed to by the Parties in writing. Paymentus shall provide adequate documents to the Client to show PCI compliance at least annually and subsequent to any changes that may impact the PCI compliance status.

3 Compensation

3.1 No Cost Installation

Paymentus will charge no fees related to the initial setup and personalization of its standard service for both Web and IVR interfaces. Paymentus shall also provide, at no cost, the conversion of its standard service for both Web and IVR interfaces to the Client's new utility billing system.

3.2 Paymentus Service Fee to User

Paymentus will charge each User a service fee for each transaction processed (hereinafter called "Paymentus Service Fee"). Such Paymentus Service Fee is to be collected in addition to the corresponding Payment as part of the transaction.

For each payment, the Paymentus Service Fee collected will be used to pay the corresponding Credit Card transaction fees or transaction fees associated with Debit Cards or eChecks (hereinafter called "Transaction Fees"). No Transaction Fees shall be passed through to Client.

A schedule of Paymentus Service Fees is attached hereto as Schedule A. The Paymentus Service Fee is based on the Average Bill Amount of $210.00 ("Fee Assumptions"). Paymentus can amend this schedule upon 30 day prior written notice to the Client, if such change is required due to changes in the Visa and MasterCard regulations or changes in Credit Card fees by more than 5% or the Average Bill Amount exceeds $210 for more than six (6) consecutive months.

3.3 Charges to Client

Paymentus shall invoice Client monthly $2.80 for each ACH / e-check transaction.

Paymentus shall charge Client a one time fee of twelve cents ($0.12) per paperless bill that is sent via the Paymentus portal.

Paymentus shall provide to Client at no cost the first seventy thousand (70,000) outbound call minutes and for the seven thousand (7,000) text message transactions per calendar year. If in any given calendar year, usage exceeds the amounts provided at no cost, additional outbound minutes shall be invoiced at eighteen ($0.18) cents per call out minute and seven ($0.07) cents per text message. Any call under thirty (30) seconds shall be invoiced at thirty (30) seconds. Calls in excess of thirty (30) seconds will be billed in six (6) second increments. All cost shall be rounded to the nearest cent. There shall be no fee charged for calls that do not connect.

4 Payment Processing

4.1 Integration with Client's Billing System

At no cost to Client, Paymentus shall develop one (1) secure and encrypted file format interface with Client's current billing system (Sunguard/HTE) using Client's existing text file format currently used to post payments to Client's billing system. The interface shall provide for secure payment processing and bill presentment consistent with Payment Card Industry Data Security Standards, State and Federal Law, and data security standards recommended by the National Institute of Standards and Technology. Client will be responsible to provide Paymentus with the one file format specification and will cooperate with Paymentus during the development of the said interface. Also at no cost to Client, Paymentus shall provide a secure and encrypted file format interface to the Clients new billing software, Advanced Utilities CIS Infinity V4. Paymentus shall work with Client's CIS software provider, N. Harris Computer Corporation,, to build, test, and successfully implement standard secure and encrypted Application Program Interface for secure payment processing and bill presentment consistent with Payment Card Industry Data Security Standards, State and Federal Law, and data security standards recommended by the National Institute of Standards and Technology. Client shall fully cooperate with Paymentus and provide input and assistance in facilitating the interface between Advanced Utilities and Paymentus.

4.2 Explicit User Confirmation

Paymentus shall confirm the dollar amount of all Payments and the corresponding Paymentus Service Fee to be charged to a Card and electronically obtain the User approval of such charges prior to initiating Card authorizations transaction. Paymentus shall provide User with electronic confirmation of all transactions.

4.3 Merchant Account

Paymentus shall arrange for the Client to have a merchant account(s) with the Paymentus Authorized Processor for processing and settlement of the credit card transactions.

4.4 Payment Authorization

For authorization purposes, Paymentus will electronically transmit all Card transactions to the appropriate Card-processing center, in real time as the transactions occur. Paymentus shall ensure that all bank card, ACH banks approval and credit card data information is secured and encrypted. Paymentus shall utilize tokenization for secure card-on-file transactions which meet or exceed the requirements of PCI DSS portal communication standards.

4.5 Settlement

Paymentus together with its authorized Card processor shall forward the Payments and corresponding Paymentus Service Fee to the appropriate card organizations for settlement. The Payment Amount for debit/credit card shall be deposited directly to the Client's depository bank account previously designated by the Client (hereinafter the "Client Bank Account"). The Payment Amount and Service Fee for ACH/e-check transactions shall be deposited into the Client Bank Account.

Paymentus together with Paymentus Authorized Processor shall continuously review its settlement and direct debit processes, its software and services for its simplicity and efficiencies and for data and security breaches and weaknesses. Any changes to the invoicing process shall be mutually agreeable to the Parties and documented in writing.

4.6 Reversed or Chargeback Transactions

With respect to all Reversed or Chargeback Transactions the Client authorizes Paymentus and Paymentus' Authorized Processor to debit the Client's Bank Account for the Payment Amount and Paymentus shall refund to the Card organization for credit back to the User the corresponding Paymentus Service Fees.

Paymentus together with Paymentus Authorized Processor will continuously review its processes for Reversed or Chargeback transactions, for simplicity and efficiencies. Any changes to the invoicing process shall be mutually agreeable to the Parties and documented in writing.

5 General Conditions of Services

5.1 Service Reports

Paymentus shall provide Client with access to electronic reports summarizing use of the Services by Users for a given reporting period.

5.2 User Adoption Communication by Client

Client will make Paymentus' Services available to its residential and commercial Clients by different means of Client communication including a) through bills, invoices and other notices; b) by providing IVR and Web payment details on the Client's website including a "Pay Now" or similar link on a prominent place on the web site; c) through Client's general IVR/Phone system; and d) other channels deemed appropriate by the Client.

Paymentus shall provide Client with logos, graphics and other marketing materials for Client's use in its communications with its users regarding the Services and/or Paymentus.

Both parties agree that Paymentus will be presented as a payment method option. Client will communicate Paymentus option to its end residential and commercial utility customers.

5.3 Independent Contractor

Client and Paymentus agree and understand that the relationship between both parties is that of an independent contractor.

5.4 Client's Responsibilities

In order for Paymentus to provide Services outlined in this Agreement, the Client shall co-operate with Paymentus by:

(i) Client will enter into all applicable merchant Card or cash management agreements, acceptable to Client.

(ii) For the duration of this Agreement, Client will keep a bill payment link connected to Paymentus System at a prominent location on the Client's website. The phone number for the IVR payment will also be added to the web site. Client will also add the IVR payment option as part of the Client's general phone system.

(iii) User Adoption marketing as described in 5.2.

(iv) Within 30 days of the merchant account setup, Client will launch the service to the Users.

(v) For the purpose of providing Client a posting file for posting to Client's billing system, Client will provide the file format specification currently used to post its payments to the current billing system. Client will fully cooperate with Paymentus and provide the information required to integrate with Client's new billing system.

6 Governing Laws

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

7 Miscellaneous Clauses

7.1 Authorized Representative

Each Party shall designate in writing an individual to act as a representative for the respective Party, with the authority to transmit instructions and receive information. The Parties, by written notice, may from time to time designate other individuals or change the individuals.

7.2 Notices

All notices of any type hereunder shall be in writing and shall be given by Certified Post or a national Courier or by hand delivery to an individual authorized to receive mail for the below listed individuals, all to the following individuals at the following locations:

To Client:

C/O: Cale Turner
701 E. Broadway
PO Box 6015
Columbia, MO 65205
Phone: 573-874-7375

To Paymentus:

C/O: President and CEO
13024 Ballantyne Corporate Place
Suite 400
Charlotte, NC 28277
Phone: 888-212-2027
Fax: 704-322-3776

Notices shall be declared to have been given or received on the date the notice is physically received if given by hand delivery or if notices given by US Post, then notice shall be deemed to have been given upon date said notice was deposited in the mail addressed in the manner set forth above. Any Party hereto by giving notice in the manner set forth herein may unilaterally change the name of the person to whom notice is to be given or the address at which the notice is to be received.

7.3 Amendment of Agreement

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

7.4 Severability

If a word, sentence or paragraph herein shall be declared illegal, unenforceable, or unconstitutional, the said word, sentence or paragraph shall be severed from this Agreement, and this Agreement shall be read as if said word, sentence or paragraph did not exist.

7.5 Attorney's Fees

Should any litigation arise concerning this Agreement between the parties hereto, the parties agree to bear their own costs and attorney's fees.

7.6 Confidentiality

Client is subject to the Missouri Sunshine Law. The Parties agree that the Agreement shall be interpreted in accordance with the provisions of the Missouri Sunshine Law, as amended. Paymentus shall maintain the confidentiality of information and records which are not subject to public disclosure under the Sunshine Law. Paymentus shall not disclose to any third party or use for any purpose inconsistent with this Agreement any confidential User information it receives in connection with its performance of the services. Paymentus shall not give any confidential or proprietary information to the Client to maintain. If it is required under this Agreement or by law that the Client maintain any confidential or proprietary information or documents about Paymentus' business, operations, financial condition, technology, systems, no-how, products, services, suppliers, clients, marketing data, plans, and models, and personnel, the documents and information shall be clearly marked as such.

7.7 Intellectual Property

In order that the Client may promote the Services and Paymentus' role in providing the Services, Paymentus grants to Client a revocable, non-exclusive, royalty-free, license to use Paymentus' logo and other service marks (the "Paymentus Marks") for such purpose only. Client does not have any right, title, license or interest, express or implied in and to any object code, software, hardware, trademarks, service mark, trade name, formula, system, know-how, telephone number, telephone line, domain name, URL, copyright image, text, script (including, without limitation, any script used by Paymentus on the IVR or the WebSite) or other intellectual property right of Paymentus ("Paymentus Intellectual Property"). All Paymentus Marks, Paymentus Intellectual Property, and the System and all rights therein (other than rights expressly granted herein) and goodwill pertain thereto belong exclusively to Paymentus.

7.8 Force Majeure

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

7.9 Data Security

a. Paymentus further covenants that any data entered into the software from the Client, its employees or Users or derived therefrom (hereinafter "City Data") shall be stored in the United States of America. City Data shall not be transferred, moved, or stored to or at any location outside the United States of America. City Data shall be confidential and proprietary information belonging to either the City or its customers or users of the Software. Paymentus shall not sell or give away any such City Data.

b. Paymentus shall maintain the security of City Data and that of Client and any User that is stored in or in any way connected with Software Products and applications and services. If either Party believes or suspects that security has been breached or City Data compromised whether it be from harmful code or otherwise, the Party shall notify the Other Party of the issue or possible security breach within forty-eight (48) hours.

c. NO HARMFUL CODE: Paymentus warrants that the Software Products do not contain Harmful Code. For purposes of this Agreement, "Harmful Code" is any code containing any program, routine, or device which is designed to delete, disable, deactivate, interfere with or otherwise harm any software, program, data, device, system or service, including without limitation, any time bomb, virus, drop dead device, malicious logic, worm, Trojan horse or trap or back door. Contractor shall include in contracts with any subcontractor a provision which prohibits the use of Harmful Code. Paymentus shall include a similar provision in its contract with subcontractors.

d. Password Security: Paymentus warrants that no 'back door' password or other method of remote access into the software code exists. Paymentus agrees that any and all access to any software code residing on the Client's client/server must be granted by the Client to Paymentus, at the Client's sole discretion.

e. RED FLAG Compliance: Paymentus' Software shall at all times comply with the terms of this Agreement, the Contract Documents, Good Financial Industry and Accounting Practices, Applicable Laws, Client's Red Flag Policy, SAS70 auditing standards, and the Client's Cloud Computing Requirements (attached as Attachment B). Paymentus shall comply with the Client's Red Flag policy and timely report any Red Flags to the Client's Program Administrator. Said report shall include Red Flags detected by Paymentus or its subcontractors or subsidiaries and Paymentus' response to the Red Flags so detected. Paymentus shall provide Client with a copy of its existing Red Flag policies and procedures, and shall promptly provide copies of any changes to its Red Flag policies and procedures.

f. Compliance with Applicable Regulations and Standards for the use, storage or processing of Credit and Debit Cards (PCI Compliance): Paymentus shall comply and shall warrant that the Paymentus software and services (including any modifications, customizations or interfaces) comply with the Payment Card Industry (PCI) Data Security Standards and the rules and regulations of payment card industry organizations including Visa, MasterCard, Discover, and any other applicable payment card industry organizations. Contractor shall further warrant that such software and/or modules be in compliance with Good Financial Industry and Accounting Practices; SAS70 auditing standards; NACHA (The Electronic Payments Association) Operating Rules; and the Client's Red Flag Policy as applicable. Paymentus shall further require that any subcontractor's software, modules, or upgrades be in compliance with this section in its contracts with those subcontractors or third party software providers. Compliance is required to be maintained with all listed applicable regulations, standards, etc. as they are updated and modified over the time period of the agreements. Paymentus shall notify Client promptly of their failure or subcontractor's failure to maintain such compliance. In addition to Paymentus' hold harmless agreement, Paymentus shall be required to bear the cost of any fees, penalties, or costs accrued to Client because of such failure to maintain such compliance.

g. Paymentus software and services shall comply with NIST recommended encryption and cyber security protocols and procedures.

8 Indemnification

8.1 Paymentus Indemnification and Hold Harmless

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

8.2 Warranty

Paymentus warrants that Paymentus and its software and services comply with the Payment Card Industry (PCI) Data Security Standards and the rules and regulations of payment card industry organizations including Visa, MasterCard, Discover, and any other applicable payment card industry organizations. Paymentus warrants that Paymentus is in compliance with and will maintain Client Data in compliance with Good Financial Industry and Accounting Practices; SAS70 auditing standards; NACHA (The Electronic Payments Association) Operating Rules; and the Client's Red Flag Policy (attached as Attachment B) as applicable.

9 Term and Termination

9.1 Term

The term of this Agreement shall commence on the effective date of this Agreement and continue for a period of 2 (two) years ("Initial Term") from the Effective Date. Services under this Agreement shall begin within thirty (30) days of the merchant account setup.

At the end of the Initial Term, this Agreement will automatically be renewed for eight (8) additional one (1) year periods unless either Client or Paymentus provide the other Party with not less than 2 (two) months prior written notice before such renewal date that such Party elects not to renew the terms of this Agreement.

9.2 Material Breach

A material breach of this Agreement shall be cured within thirty (30) days ("Cure Period") after a party notifies the other of such breach. In the event, such material breach has not been cured within the Cure Period, the non-breaching party can terminate this Agreement by providing the other party with such written notice of termination.

9.3 For Convenience

Either Party may terminate this Agreement at any time upon sixty (60) day written notice to the other party.

9.4 Termination by Mutual Agreement

The Agreement may be terminated at any time during its Term upon mutual agreement by both Parties.

9.5 Upon Termination

Upon termination of this Agreement, the Parties agree to cooperate with one another to ensure that all Payments are accounted for and all refundable transactions have been completed. Upon termination, Paymentus shall cease all Services being provided hereunder.

9.6 Termination Due to Cyber Security Threat or Attack

Notwithstanding the foregoing, Client may take whatever action Client deems necessary to protect itself and its Users from a cyber security threat or attack, including but not limited to immediate termination of the Agreement.

10. General Terms and Conditions

10.1 Employment of Unauthorized Aliens Prohibited

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

10.2 Insurance Requirements

Paymentus shall maintain, on a primary basis and at its sole expense, at all times during the life of the Agreement the following insurance coverages, limits, including endorsements described herein. The requirements contained herein, as well as the Client's review or acceptance of insurance maintained by Paymentus is not intended to, and shall not in any manner limit or qualify the liabilities or obligations assumed by Paymentus under the Agreement. Coverage to be provided as follows by a carrier with A.M. Best minimum rating of A- VIII.

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

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

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

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

e. Professional Liability. Paymentus shall maintain Professional (Errors and Omissions) Liability at a limit of liability not less than $2,000,000.00 per occurrence. When a self-insured retention (SIR) or deductible exceeds $10,000.00, the Client reserves the right, but not the obligation to review and request a copy of Paymentus' most recent annual report or audited financial statement. For policies written on a "Claims-Made" basis, Paymentus agrees to maintain a Retroactive Date prior to or equal to the Effective Date of this Agreement. In the event the policy is canceled, non-renewed, switched to an Occurrence Form, retroactive date advanced; or any other event triggering the right to purchase a Supplemental Extended Reporting Period (SERP) during the life of this Agreement, Paymentus agrees to purchase a SERP with a minimum reporting period not less than two (2) years. The requirement to purchase a SERP shall not relieve Paymentus of the obligation to provide replacement coverage.

f. The City of Columbia, its elected officials and employees are to be Additional Insureds with respect to its Commercial General Liability Insurance. A certificate of insurance evidencing all coverage required is to be provided at least 10 days prior to the Effective Date of the Agreement between the Paymentus and the Client. Paymentus is required to maintain coverages as stated and required to notify the Client of a Carrier Change or cancellation within two (2) business days. The Client reserves the right to request a copy of the policy.

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

h. Failure to maintain the required insurance in force may be cause for termination of the Agreement. In the event Paymentus fails to maintain and keep in force the required insurance or to obtain coverage from its subcontractors, the Client shall have the right to cancel and terminate the Agreement without notice.

i. The insurance required by the provisions of this article is required in the public interest and the Client does not assume any liability for acts of the Paymentus and/or their employees and/or their subcontractors in the performance of this Agreement.

10.3 Nature of Client's Obligations

The obligations of the Client under this Agreement, which require the expenditures of funds, shall be conditional obligations, subject to the availability of funds appropriated for the purpose.

10.4 No Assignment

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

10.5 No Third-Party Beneficiary

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

10.6 General Laws

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

10.7 No Waiver of Immunities

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

10.8 Professional Oversight Indemnification

Paymentus understands and agrees that Client has contracted with Paymentus based upon Paymentus' representations that Paymentus is a skilled professional and fully able to provide the services set out in this Agreement. In addition to any other indemnification set out in this Agreement, Paymentus agrees to defend, indemnify and hold and save harmless the Client from any and all claims, settlements and judgments whatsoever arising out of Client's alleged negligence in hiring or failing to properly supervise Paymentus. The insurance required by this Agreement shall include coverage which shall meet Paymentus' obligations to indemnify the Client as set out above and Client shall be named as additional insured for such insurance.

10.9 Equal Opportunity Employment/Nondiscrimination

It is the policy of the Client that all contractors who provide goods and services to the Client by contract/agreement, shall, as a condition of providing goods and services, adhere to all Federal, State and Local laws, ordinances, rules and regulations, and policies, and if applicable, prohibiting discrimination in regard to persons to be served and employees and applicants for employment including, but not limited to, the following: (a) Section 504 of the Federal Rehabilitation Act of 1973, PL 93-112, 87 Stat 355, as amended, and rules adopted thereunder; (b) The Americans with Disabilities Act of 1990, PL 101-336, 104 Stat 327 (42 USCA 12101 et seq.), as amended, and regulations promulgated thereunder; (c) Equal Employment Opportunity including Title VI of the Civil Rights Act of 1964, and the regulations promulgated thereunder; and (d) Chapter 12 of the City of Columbia's Code of Ordinances. Paymentus shall, as a condition of providing goods and services, as required by state and federal law and the City's Equal Opportunity Employment/Nondiscrimination ordinance, not discriminate against persons to be served or an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment because of race, color, religion, national origin, age, sex, sexual orientation, gender identity, ancestry or disability.

10.10 Compliance with Americans with Disabilities Act

Paymentus represents and warrants that its software and services are and shall remain compliant with the Americans with Disabilities Act and regulations relating to accessibility.

10.11 Contract Documents

This Agreement includes the following exhibits, which are incorporated herein by reference:

Attachment/Exhibit	Description
A	Paymentus Service Fee Schedule
B	City of Columbia's Red Flag Policy and Cloud Computing Requirements

In the event of a conflict between the terms of an exhibit or attachment and the terms of this Agreement, the terms of this Agreement controls.

10.12 Entire Agreement

This Agreement represents the entire and integrated Agreement between Paymentus and Client relative to the Scope of Services herein. All previous or contemporaneous agreements, representations, promises and conditions relating to Paymentus' services described herein are superseded.

[SIGNATURES ON THE FOLLOWING PAGE]

IN WITNESS WHEREOF, the Parties have hereunto executed this Agreement in triplicate the day and the year of the last signatory noted below.

CITY OF COLUMBIA, MISSOURI

By: ______________________________
Mike Matthes, City Manager

Date: ______________________________

ATTEST:

By: ______________________________
Sheela Amin, City Clerk

APPROVED AS TO FORM:

By: ______________________________
Nancy Thompson, City Counselor

PAYMENTUS CORPORATION

By: ______________________________

Title: V.P.

Date: 4-5-2016

ATTEST:

By: Theresa L Bentley

Name: Theresa L. Bentley

Title: Senior Acct. Mgr.

Schedule A – Paymentus Service Fee Schedule

Paymentus Service Fee charged to the User will be based on the following table:

Payment Type	Paymentus Service Fee
Utility Payments	
• Residential Credit/Debit/ACH	$3.55 per payment – Maximum amount per payment is $750 (Multiple payments can be made)
• Commercial Credit/Debit/ACH	$4.60 per payment – Maximum amount per payment is $1,000 (Multiple payments can be made)

The Paymentus Service Fees will be collected in addition to the end-user bill payment total.

Exhibit B

CHASE ™
Paymentech

SUBMITTER MERCHANT
PAYMENT PROCESSING INSTRUCTIONS AND GUIDELINES
(For use by Paymentus' U.S.-based clients)

Paymentech, LLC ("*Paymentech*" or "we", "us" or "our" and the like), for itself and on behalf of JPMorgan Chase Bank, N.A. ("Member"), is very excited about the opportunity to join **Paymentus Corporation** in providing you with state-of-the-art payment processing services. When your Customers pay you through Paymentus Corporation, you may be the recipient of a Card funded payment. The organizations that operate these Card systems (such as Visa U.S.A., Inc. and MasterCard International Incorporated; collectively, the "Payment Brands") require that you (i) enter into a direct contractual relationship with an entity that is a member of the Payment Brand and (ii) agree to comply with Payment Brand Rules as they pertain to applicable Card Transaction you submit through Paymentus Corporation. You are also required to fill out an Application with Paymentech. The Application provides Paymentech with information relative to your processing practices and expectations.

By executing this document, you are fulfilling the Payment Brand Rule of entering into a direct contractual relationship with a member, and you are agreeing to comply with Payment Brand Rules as they pertain to Transactions you submit for processing through the Paymentus Corporation service. We understand and acknowledge that you have contracted with Paymentus Corporation to obtain Card processing services on your behalf and that Paymentus Corporation may have agreed to be responsible for your obligations to us for such Transactions and as set forth in these guidelines.

The following information is designed to inform and assist you as we begin our relationship.

1. Your Acceptance of Cards

- You agree to comply with all Payment Brand Rules, as may be applicable to you and in effect from time. You understand that we may be required to modify these instructions and guidelines in order to comply with requirements imposed by the Payment Brands.
- In offering payment options to your customers, you may elect any one of the following options. These acceptance options above apply only to domestic transactions:

  (1) Accept ***all*** types of Visa and MasterCard cards, including consumer credit and debit/check cards, and commercial credit and debit/check cards;
  (2) Accept ***only*** Visa and MasterCard credit cards and commercial cards (If you select this option, you must accept all consumer credit cards (but not consumer debit/check cards) and all commercial card products, including business debit/check cards); or
  (3) Accept ***only*** Visa and MasterCard consumer debit/check cards (If you select this option, you must accept all consumer debit/check card products (but not business debit/check cards) and refuse to accept any kind of credit cards).

- If you choose to limit the types of Visa and MasterCard cards you accept, you must display appropriate signage to indicate acceptance of the limited acceptance category you have selected (that is, accept only debit/check card products or only credit and commercial products).
- For recurring transactions, you must obtain a written request or similar authentication from your Customer for the goods and/or services to be charged to the Customer's Card, specifying the frequency of the recurring charge and the duration of time during which such charges may be made.

2. Settlement

- Upon our receipt of your Transactions, we will process your Transactions to facilitate the funds transfer between the various Payment Brands, you and Paymentus Corporation. Unless otherwise agreed to by the parties, after we receive credit for such Transactions, we will provide provisional credit to one or more of the Bank Account(s) you designate herein under the "Funding Schedule" section.
- You must not submit Transactions for payment until the goods are delivered, shipped, or the services are performed. If a Customer disputes being charged for merchandise or services before receiving them, the result may be a Chargeback to you.

3. *Chargebacks*

- You may receive a Chargeback for a number of reasons. The following are some of the most common reasons for Chargebacks, but in no way is this meant to be an exhaustive list of all Chargeback reasons:
  (1) You do not issue a refund to a Customer upon the return or non-delivery of goods or services;
  (2) An authorization/approval code was required and not obtained;
  (3) The Transaction was fraudulent;
  (4) The Customer disputes the Card sale or the signature on the sale documentation, or claims that the sale is subject to a set-off, defense or counterclaim; or
  (5) The Customer refuses to make payment for a Card sale because in the Customer's good faith opinion, a claim or complaint has not been resolved, or has been resolved by you but in an unsatisfactory manner.

4. *Data Security and Privacy*

- By signing below, you represent to us that you **do not** have access to any Card Information (such as the Customer's primary account number, expiration date, security code or personal identification number) and you will not request access to such Card Information from Paymentus Corporation. In the event that you do happen to receive Card Information in connection with the processing services provided by Paymentus Corporation or Paymentech under these guidelines, you agree that you will not use it for any fraudulent purpose or in violation of any Payment Brands or applicable law and you will comply with all applicable Payment Brand Rules and Security Standards. If at any time you believe that Card Information has been compromised, you must notify us promptly and assist in providing notification to the proper parties. You must ensure your compliance with all Security Standards that are applicable to you and which may be published from time to time by the Payment Brands. If any Payment Brand requires an audit of you due to a data security compromise event or suspected event, you agree to cooperate with such audit. You may not use any Card Information other than for the sole purpose of completing the Transaction authorized by the Customer for which the information was provided to you, or as specifically allowed by Payment Brand Rules, or required by law. In the event of your failure, including bankruptcy, insolvency or other suspension of business operations, you shall not sell, transfer or disclose any materials that contain Transaction information or Card Information to third parties.

5. *Funding Schedule*

- In order to receive funds from Paymentech, you must maintain one or more bank account(s) at a bank that is a member of the Automated Clearing House ("ACH") system and the Federal Reserve wire system (the "Bank Account"). You must designate at least one Bank Account for the deposit and settlement of funds and the debit of any fees and costs associated with Paymentech's processing of the Transactions (all such designated Bank Accounts shall be collectively referred to herein as the "Settlement Account"). You authorize Paymentech to initiate electronic credit and debit entries and adjustments to your Settlement Account in accordance with this Section 5. We will not be liable for any delays in receipt of funds or errors in Settlement Account entries caused by third parties, including but not limited to delays or errors by the Payment Brands or your bank.

- Unless otherwise agreed to by the parties, the proceeds payable to the Settlement Account shall be equal to the amounts received by us in respect of your Card transactions less all Chargebacks, Customer refunds and other applicable charges. Such amounts will be paid into the Settlement Account promptly following our receipt of the funds. If the proceeds payable to the Settlement Account do not represent sufficient credits, or the Settlement Account does not have a sufficient balance to pay amounts due from you under these guidelines, we may pursue one or more of the following options: (i) demand and receive immediate payment for such amounts; (ii) debit a Bank Account for the amount of the negative balance; (iii) withhold settlement payments to the Settlement Account until all amounts are paid, (iv) delay presentation of refunds until a payment is made to us of a sufficient amount to cover the negative balance; and (v) pursue any remedies we may have at law or in equity.

- Unless and until we receive written instructions from you to the contrary, all amounts payable by Paymentech to you will be deposited in the Settlement Account designated and authorized by you as set forth below:

Name of Bank: ______________________________

ABA No.: ______________________________

Account No.: ______________________________

Account Name: ______________________________

Reference: ______________________________

6. ***Convenience Fee Transactions.*** You and Paymentus Corporation hereby agree that

- All Convenience Fee Transactions will be submitted by Paymentus Corporation to Paymentech under that certain Submitter Agreement entered into by and between Paymentus Corporation and Paymentech; and
- All Card transactions will be submitted by Paymentus Corporation on your behalf to Paymentech under the terms of these Payment Processing Instructions and Guidelines.

7. ***Definitions***

"***Application***" is a statement of your financial condition, a description of the characteristics of your business or organization, and related information you have previously or concurrently submitted to us, including credit and financial information.

"***Card***" is an account, or evidence of an account, authorized and established between a Customer and a Payment Brand, or representatives or members of a Payment Brand that you accept from Customers as payment for a good or service. Payment Instruments include, but are not limited to, credit and debit cards, stored value cards, loyalty cards, electronic gift cards, authorized account or access numbers, paper certificates and credit accounts.

"***Chargeback***" is a reversal of a Transaction you previously presented to Paymentech pursuant to Payment Brand Rules.

"***Convenience Fee Transaction***" is a Transaction representing a charge to a customer's Card for the convenience of using the payment channel offered by you and Paymentus Corporation.

"***Customer***" is the person or entity to whom a Card is issued or who is otherwise authorized to use a Payment Instrument.

"***Member***" is JPMorgan Chase Bank, N.A. or other entity providing sponsorship to Paymentech as required by all applicable Payment Brand. Your acceptance of Payment Brand products is extended by the Member.

"***Payment Brand***" is any payment method provider whose payment method is accepted by Paymentech for processing, including, but not limited to, Visa, U.S.A., Inc., MasterCard International, Inc., Discover Financial Services, LLC and other credit and debit card providers, debit network providers, gift card and other stored value and loyalty program providers. Payment Brand also includes the Payment Card Industry Security Standards Council.

"***Payment Brand Rules***" are the bylaws, rules, and regulations, as they exist from time to time, of the Payment Brands.

*"**Card Information**"* is information related to a Customer or the Customer's Card, that is obtained by you or Paymentus Corporation from the Customer's Card, or from the Customer in connection with his or her use of a Card (for example a security code, a PIN number, or the customer's zip code when provided as part of an address verification system). Without limiting the foregoing, such information may include a the Card account number and expiration date, the Customer's name or date of birth, PIN data, security code data (such as CVV2 and CVC2) and any data read, scanned, imprinted, or otherwise obtained from the Payment Instrument, whether printed thereon, or magnetically, electronically or otherwise stored thereon.

"***Paymentech***", "***we***", "***our***", and "***us***" is Paymentech, LLC, a Delaware limited liability company, having its principal office at 14221 Dallas Parkway, Dallas, Texas 75254.

"***Security Standards***" are all rules, regulations, standards or guidelines adopted or required by the Payment Brands or the Payment Card Industry Security Standards Council relating to privacy, data security and the safeguarding, disclosure and handling of Payment Instrument Information, including but not limited to the Payment Card Industry Data Security Standards ("PCI DSS"), Visa's Cardholder Information Security Program ("CISP"), Discover's Information Security & Compliance Program, American Express's Data Security Operating Policy, MasterCard's Site Data Protection Program ("SDP"), Visa's Payment Application Best Practices ("PABP"), the Payment Card Industry's Payment Application Data Security Standard ("PA DSS"), MasterCard's POS Terminal Security program and the Payment Card Industry PIN Entry Device Standard, in each case as they may be amended from time to time.

"***Transaction***" is a transaction conducted between a Customer and you utilizing a Card in which consideration is exchanged between the Customer and you.

[Signature page to follow]

Please acknowledge your receipt of these instructions and guidelines and your agreement to comply therewith.

Agreed and Accepted by:

City of Columbia, Missouri
MERCHANT LEGAL NAME (Print or Type)

Address (Print or Type)

By (authorized signature)

By, Name, Title (Print or Type)

Date

Agreed and Accepted by:

Paymentus Corporation

3455 Peachtree Rd NE 5th Fl, Atlanta, GA 30326
Address (Print or Type)

By (authorized signature)

By, Name, Title (Print or Type)

Date

Agreed and Accepted by:

PAYMENTECH, LLC for itself and on behalf of
JPMORGAN CHASE BANK, N.A.

By:

Print Name:

Title:

Date:

Address: 4 Northeastern Boulevard, Salem, NH 03079

► 1 COMPANY INFORMATION

Federal regulations require that we collect and retain for our records information to verify merchant identity.

COMPANY LEGAL NAME:	City of Columbia, Missouri			**TAXPAYER ID**	43-6000810
REGISTERED TRADE NAME	N/A			**YEAR BUSINESS STARTED**	
PHYSICAL STREET ADDRESS: (NO PO BOX OR PAID MAIL BOX)	701 E. BROADWAY				
CITY	Columbia	**STATE**	MO	**ZIP CODE**	65201
PRIMARY CONTACT	Bette Wordelman			**TELEPHONE #**	573-874-7369

TYPE OF ENTITY

☑ Municipal Utility ☐ Municipality ☐ Public Utility ☐ Private Utility ☐ Public Corporation ☐ Private Corporation

☐ Govt. Agency ☐ Partnership ☐ Sole Proprietorship ☐ Non Profit ☐ OTHER:

☐ LLC* *** IF LLC, TAXED AS:** ☐ Disregarded Entity ☐ Partnership ☐ Corporation

STATE OF FORMATION	Missouri	**DATE OF FORMATION** (MM/DD/YYYY)	
TRADING SYMBOL		**FISCAL YEAR END** (MM/DD/YYYY)	
HAS MERCHANT EVER FILED BANKRUPTCY? ☐ YES ☒ NO	**IF YES, WHAT CHAPTER?**	**FILING DATE:**	**EMERGENCE DATE:**

► 2

OWNERS (Ownership is not required if you are a public entity, non-profit, or municipality. All other entity types must disclose ownership.) OWNERS MUST PROVIDE SOCIAL SECURITY NUMBER. EACH OWNER SIGNING AUTHORIZES JPMORGAN CHASE BANK N.A. AND PAYMENTECH, LLC, AS PART OF THIS INVESTIGATION, TO OBTAIN AND REVIEW THIRD PARTY CREDIT BUREAU REPORTS ON SUCH OWNER. OWNERSHIP DETAILS MUST BE PROVIDED FOR EACH INDIVIDUAL OR LEGAL ENTITY OWNER WITH A 10% OR GREATER OWNERSHIP INTEREST.

NAME		**SOCIAL SECURITY OR TAX ID NUMBER**		**BIRTHDATE OR DATE OF INCORPORATION**	
STREET ADDRESS				**TELEPHONE NUMBER**	
CITY		**STATE**		**ZIP CODE**	
SIGNATURE				**PERCENT OWNERSHIP**	%

NAME		**SOCIAL SECURITY OR TAX ID NUMBER**		**BIRTHDATE OR DATE OF INCORPORATION**	
STREET ADDRESS				**TELEPHONE NUMBER**	
CITY		**STATE**		**ZIP CODE**	
SIGNATURE				**PERCENT OWNERSHIP**	%

DO YOU HAVE ANY ADDITIONAL OWNERS (NOT LISTED ABOVE) THAT HAVE 10% OR GREATER OWNERSHIP?

☐ **YES OWNER ADDENDUM REQUIRED (SALES REPRESENTATIVE WILL PROVIDE)** ☐ **NO**

► 3 OFFICERS

COMPANY PRESIDENT:	Mike Matthes, City Manager	**COMPANY CFO:**	Michele Nix

IS THERE ANYONE NOT LISTED ABOVE WHO HAS THE AUTHORITY TO MAKE FINANCIAL DECISIONS OR CONTROL COMPANY POLICY ON BEHALF OF YOUR BUSINESS?

☑ **YES OWNER ADDENDUM REQUIRED (SALES REPRESENTATIVE WILL PROVIDE)** ☐ **NO**

▶ 4 AUTHORIZED ADMINISTRATOR FOR ACCOUNT BOARDING AND IMPLEMENTATION

AUTHORIZED ADMINISTRATOR FOR PURPOSES OF ACCOUNT BOARDING AND IMPLEMENTATION MEANS AN OWNER, PARTNER, OFFICER, EMPLOYEE OR OTHER AGENT OF THE MERCHANT THAT HAS BEEN APPOINTED BY AN EXECUTIVE OF MERCHANT AND WHO IS DULLY AUTHORIZED TO PROVIDE INFORMATION AND EXECUTE DOCUMENTATION ON BEHALF OF AND RELATED TO MERCHANT IN ORDER TO FACILITATE THE INITIAL SET UP OF MERCHANTS'S ACCOUNT WITH CHASE PAYMENTECH. PER CHASE PAYMENTECH POLICY, AUTHORIZED ADMINISTRATORS ARE NOT PERMITTED TO MODIFY THE MERCHANT'S ACCOUNT WITH CHASE PAYMENTECH AFTER COMPLETION OF THE INITIAL SET UP OF MERCHANTS'S ACCOUNT. SUCH CHANGES MUST BE MADE, BY AN EXECUTIVE OR FINANCIAL CONTACT, AS APPLICABLE AND AS THOSE ROLES ARE DEFINED BY MERCHANT.

NAME (please print)	Bette Wordelman	**TITLE** (please print)	TreasureR
TELEPHONE NUMBER	573-874-7369	**EMAIL ADDRESS:**	Bette.WoRdelman@como.gov
SIGNATURE		**DATE:**	

▶ 5 CERTIFICATION

I, the undersigned, being an officer/principal of City of Columbia, MO **represent and warrant that the statements made on this document are correct and factual. JPMorgan Chase Bank, N.A ("Member") and Paymentech, LLC ("Paymentech" or "Chase Paymentech") are authorized to conduct any necessary investigation, including without limitation, authorization for a bank to release standard banking information.**

(Photocopy of signature below is valid for the release of information and will remain valid until the termination or expiration of the Merchant Agreement)

NAME (please print)		**TITLE** (please print)	
SIGNATURE		**DATE**	

PAYMENTECH INTERNAL USE ONLY

SUBMITTER NAME	**Paymentus Corporation**

***Note: Each Merchant is required to submit a W9 with this application, regardless if Paymentech will be utilizing the Submitter's TIN for IRS reporting purposes.**

CHASE
Paymentech

Owner/Officer Addendum

(used for additional/beneficial owners)

Rev. OWNEROFFICER 11/2015

This Addendum supplements the Merchant Application And/or Agreement executed and submitted by City of Columbia, Missou (Merchant Legal Name - "Merchant"). As such, this Addendum shall (i) be deemed incorporated into and a part of Merchant's Application to establish a Merchant account with Paymentech, LLC and JPMorgan Chase Bank, N.A. and (ii) in accordance with such Merchant Application and Agreement, constitute a part of the entire Agreement governing all Merchant accounts.

Merchant indicated on its application additional owners with 10% or greater ownership or additional representatives that have authority to make financial decisions or influence policy on behalf of your business. Please list their information below and indicate if they are an Owner or Representative. (Attach additional pages if needed)

Owner	- Individual or entity that owns 10% or greater of the Merchant, either directly or indirectly
Direct Owner	- Refers to an individual or entity with direct ownership of the entity in section one of the Merchant Application (The Applicant)
Indirect Owner	- Has ownership of the applicant through ownership in another entity which is a direct or indirect owner of The Applicant
Key Decision Maker	- Individual empowered to make financial or business decisions on behalf of Merchant
Voting Member of Board of Directors (or Board of Trustees, or other Governing Board)	- Individuals with voting rights chosen to govern the affairs of Merchant
Senior manager	- Employee that can make policy and financial decisions on behalf of Merchant
Authorized Representative	- Representative that has signing authority on Merchant accounts

1 Name of Individual or Entity: (if individual please provide residential address below) Lynn Cannon	Owner of (entity name)		□ **OWNER** (reference diagram below)
Street Address (No PO Box or paid mailbox) 701 E. Broadway			____ % ownership
City Columbia	State MO	Zip Code 65201	☒ **REPRESENTATIVE**
Title Assistant Finance Director	Country of Domicile US		

2 Name of Individual or Entity: (if individual please provide residential address below)	Owner of (entity name)		□ **OWNER** (reference diagram below)
Street Address (No PO Box or paid mailbox)			____ % ownership
City	State	Zip Code	□ **REPRESENTATIVE**
Title	Country of Domicile		

3 Name of Individual or Entity: (if individual please provide residential address below)	Owner of (entity name)		□ **OWNER** (reference diagram below)
Street Address (No PO Box or paid mailbox)			____ % ownership
City	State	Zip Code	□ **REPRESENTATIVE**
Title	Country of Domicile		

(Attach additional pages if needed)

(Continues on next page)

I, the undersigned, certify:

- that I am an owner, partner, officer or other authorized representative of the Merchant ("Authorized Representative") and
- that I am duly authorized to enter into this agreement~~s~~ on behalf of Merchant and to legally bind Merchant to such agreement~~s~~.
- that I am duly authorized to submit this Addendum and all information contained herein on behalf of the Merchant.

By submitting this Addendum, Merchant, through the undersigned Authorized Representative

- represents and warrants that the person submitting this Addendum is duly authorized to enter into this agreement~~s~~ on behalf of Merchant and to legally bind Merchant to such agreement~~s~~.
- represents and warrants that all information contained within this Addendum is true, complete and not misleading.

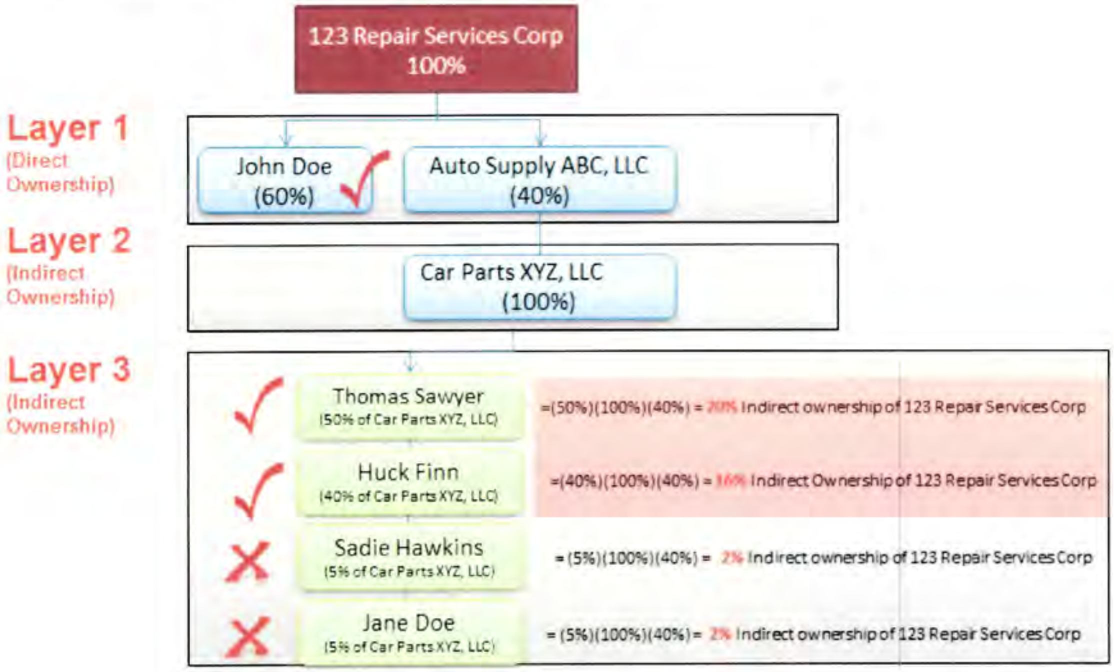
X ______________________________ ______________________________ ______________________________

Signature (Must be a signer on the Merchant Application) Print Name Date

Note: Signer must be listed as an Owner or Authorized Representative on the Merchant Application or this Owner/Officer Addendum

Example of Complex Ownership Structure

Note: Layer 1 would be Owners on the Merchant Application.
Layer 2 would be on this addendum
Layer 3 (if applicable) would be on this addendum


123 Repair Services Corp
100%
Layer 1
(Direct Ownership)
John Doe
(60%)
Auto Supply ABC, LLC
(40%)
Layer 2
(Indirect Ownership)
Car Parts XYZ, LLC
(100%)
Layer 3
(Indirect Ownership)
Thomas Sawyer
(50% of Car Parts XYZ, LLC)
=(50%)(100%)(40%) = 20% Indirect ownership of 123 Repair Services Corp
Huck Finn
(40% of Car Parts XYZ, LLC)
=(40%)(100%)(40%) = 16% Indirect Ownership of 123 Repair Services Corp
Sadie Hawkins
(5% of Car Parts XYZ, LLC)
= (5%)(100%)(40%) = 2% Indirect ownership of 123 Repair Services Corp
Jane Doe
(5% of Car Parts XYZ, LLC)
= (5%)(100%)(40%) = 2% Indirect ownership of 123 Repair Services Corp

CHASE ™
Paymentech

Government Owned Addendum

(Municipal Utilities, Municipalities, Gov't Agencies)

Rev. GOV 11/2015

This Addendum supplements the Merchant Application And/or Agreement executed and submitted by City of Columbia (Merchant Legal Name - "Merchant"). As such, this Addendum shall (i) be deemed incorporated into and a part of Merchant's Application to establish a Merchant account with Paymentech, LLC and JPMorgan Chase Bank, N.A. and (ii) in accordance with such Merchant Application and Agreement, constitute a part of the entire Agreement governing all Merchant accounts.

FUNCTION

Merchant is a Government Entity. Function of Merchant.

Municipal Utility

Authorized Purpose of Government Entity?

Authorized Representative

I, the undersigned, certify:

- that I am an officer or other authorized representative of the Merchant ("Authorized Representative") and
- that I am duly authorized to enter into this agreement~~s~~ on behalf of Merchant and to legally bind Merchant to such agreement~~s~~.
- that I am duly authorized to submit this Addendum and all information contained herein on behalf of the Merchant.

By submitting this Addendum, Merchant, through the undersigned Authorized Representative

- represents and warrants that the person submitting this Addendum is duly authorized to enter into this agreement~~s~~ on behalf of Merchant and to legally bind Merchant to such agreement~~s~~.
- represents and warrants that all information contained within this Addendum is true, complete and not misleading.

Authorized Representative:

X ______________________ ______________________ ______________

Signature | Print Name | Date

SUPPORTING
DOCUMENTS FOR
THIS AGENDA ITEM

Red Flag Rule

City of Columbia Identity Theft Prevention Program

Effective December, 2010

City Council Adopted and Effective Date: _______________

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

Table of Contents

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

IDENTIFICATION OF RED FLAGS

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

1. Notifications and Warnings from Consumer Reporting Agencies

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Suspicious Personal Identifying Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Notice Regarding Possible Identity Theft

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

DETECTION OF RED FLAGS.

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

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

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

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

    4) Independently contacting the customer; and

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

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

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

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

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

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

PREVENTING AND MITIGATING IDENTITY THEFT

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

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

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

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

4) Reopening a Record with a new number;

5) Not opening a new Record;

6) Closing an existing Record;

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

> **Example: If the City receives notice that its system has been compromised such that a customer's personal information has become accessible, at a minimum the City will notify the customer and change passwords.**
>
> **Example: If the City receives notice that a person has provided inaccurate identification information, the Record will be closed immediately and notify Law Enforcement.**

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

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

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

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

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

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

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

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

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

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

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

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

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

10) Maintaining secure office location;

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

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

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

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

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

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

UPDATING THE PROGRAM AND THE RED FLAGS

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

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

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

PROGRAM ADMINISTRATION AND TRAINING

1. Oversight.

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

2. Staff Training and Reports.

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

3. Service Provider Arrangements.

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

> 1) Requiring, by contract, that service providers have such policies and procedures in place;
>
> 2) Requiring, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator; and,
>
> 3) Each Department is required to maintain an up-to-date written internal policy as it pertains to their internal security and identity theft.

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

Appendix A

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

PURPOSE: Establish guidelines consistent with City of Columbia Ordinance

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

PROCEDURE:

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

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

Customer information on master file is password protected.

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

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

Appendix A (cont'd)

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

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

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

PROCEDURE:

Identification of Red Flags

- Mail sent to the license applicant is repeatedly returned as undeliverable.

- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the license applicant.

- Receiving information from American DataBank Inc., the company that provides criminal background check services, concerning the inconsistency of a social security number and date of birth of a license applicant.

- The license applicant fails to provide the required personal identifying information (incomplete application).

- Receiving verbal or written information concerning an applicant submitting fraudulent documents.

- Applicant's driver's license photo is inconsistent with the person presenting the documentation.

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

Detection of Red Flags

- Require identifying information from all license applicants.

- Verify the applicant’s identity in person.

- Review documentation showing the existence of a business entity.

- Verify the identity of applicants, if they request information.

Preventing and Mitigating Identity Theft

- American Databank, Inc. monitors identifying information for inconsistencies in social security number, name, date of birth, and relays this information to the Business License Office.

- The invoices received from American Databank include only the last four digits of the applicants’ social security number.

- Applicants’ social security number and business gross receipts information are always deleted/blacked out on documents requested from a licensee’s file.

- Social security and gross receipts information are never released unless requested by the applicant in person upon providing identification.

- Requests for confidential licensing information from City Police Department staff, Law Department staff, representatives from governmental agencies, etc., are required to obtain this information from the Business Services Administrator after providing identification.

- Inactive business license files are stored in a locked area.

- All Business License staff computers are password protected.

- Computer screens are only visible to the Business License employee when accessing licensing records.

- File cabinets that contain business license records, as well as hotel/motel and cigarette tax records, are locked at the end of each business day. The Business License area is never left unattended during office hours and access to this area is restricted to Business License staff and management.

- Always obtain copy of applicant’s driver’s license or other picture ID when applying for a license or permit.

- Check immigration papers to ensure validity.

- If an applicant fails to provide the requested personal identifying information, the license or permit application is denied.

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

- Double check with Missouri Secretary of State’s Office to confirm members of a corporation are consistent with those listed on the application.

- Obtain criminal background check from previous state in which the applicant resided if the applicant has lived in Missouri for less than one year.

- Computer screen darkens or fades out when staff is away from their desks.

- The Business Services Administrator is the only person who can grant access to the business license system.

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

Appendix A (cont'd)

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

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

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

PROCEDURE:

Identification of Red Flags

- Mail sent to the miscellaneous receivable customer is repeatedly returned as undeliverable.

- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the miscellaneous receivable customer.

- Receiving verbal or written information concerning a miscellaneous receivable customer submitting fraudulent documents.

- Owner of company listed on miscellaneous receivable customer inconsistent with the MO Secretary of State records.

Detection of Red Flags

- Review documentation showing the existence of a business entity.

- Verify the identity of miscellaneous receivable customer if they request information.

Preventing and Mitigating Identity Theft

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

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

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

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

- All miscellaneous receivable customer system records are password protected.

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

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

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

APPENDIX B

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

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

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

<u>PROCEDURE:</u>

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

APPENDIX C

Information Systems Internal Identity Theft Policy
Effective April 3, 2008

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

1.3 Identification and Authentication

1.3.1 Passwords

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

1.3.1.1 Complexity

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

PCI DSS 8.5.10

1.3.1.2 Rotation

Passwords should not resemble previous passwords. For example, “Password12” should not be used if “Password11” has been used before. Where possible, systems and applications should be set to “remember” old passwords and disallow use of passwords that match or are similar to a previous password. Where possible, systems should be set to store the last 10 passwords.

PCI DSS 8.5.12

1.3.1.3 Password Responsibilities of Users

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

a) Their user id must not accompany the password

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

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

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

1.3.1.4 Creating and resetting passwords

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

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

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

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

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

PCI DSS 8.5.2, PCI DSS 8.5.3

1.3.1.5 Password expire

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

PCI DSS 8.5.9

1.3.1.6 Password Transmission and Storage

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

PCI DSS 8.4

1.4.3 User privilege audits

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

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

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

Satisfies NERC CIP-003-1 R5.2

1.4.4 Account audits

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

1) Enumeration of all user accounts.

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

NERC CIP-003-1 R5.2

1.5 Accountability and risk mitigation measures

1.5.1 Accountability

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

1.5.2 Authentication logging

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

1.5.3 Review of authentication events

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

1.5.4 Last login information

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

1.6 Administration

1.6.1 Clipping level

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

PCI DSS 8.5.13, PCI DSS 8.5.14

APPENDIX D

Columbia Police Department Notification Procedures
Effective October 24, 2008

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

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

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

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

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

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

Case preparation guideline for embezzlement or internal theft cases

Major Crimes Division, Columbia Police Department

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

Document preparation:

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

Overview sheet:

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

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

Narrative sheet:

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

Itemized list

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

Supporting Documents:

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

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

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

Identity Theft Victim Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Document everything: Keep originals of all correspondence and documents; send copies as necessary

- Keep a record of everyone you talk to (names, dates, etc.)

- Keep all your files FOREVER! If something happens at a later date, you will be glad you did

- If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where it was filed. A list is available on the UST website at www.usdoj.gov/ust/

- If wrongful criminal violations are attributed to your name, contact that law enforcement agency

- Contact the Department of Motor Vehicles at www.dor.mo.gov/ and ask that your files be flagged

- If theft of mail was involved, contact the U.S. Postal Inspection Service at www.usps.gov/websites/depart/inspect

- If phone fraud was involved, contact the Public Utility Commission. If cell phone or long distance service was involved, contact the FCC at www.fcc.gov

- If your social security number was involved, contact the Social Security Administration at www.socialsecurity.gov

- If tax fraud was involved, contact the IRS at www.treas.gov/irs/ci

- **You can find much more information about Identity Theft, with more help and guidance, at the FTC's website at www.consumer.gov/idtheft**

- ***Information provided comes directly from the FTC's website at www.consumer.gov/idtheft***

Appendix E

Identity Theft Training Program
Effective December 1, 2008

Training Protocol

I. Introduction

a. What is Identity Theft?

II. Red Flag Legislation

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

III. The City's Identity Theft Prevention Program

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

IV. Identity Theft

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

V. How to Report

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

VI. Resources

Appendix F

Needs Assessment
Effective December 1, 2008

Conducting a Needs Assessment

Opening a New Record

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

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

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

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

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

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

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

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

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

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

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

11) What safeguards would you like to implement? _________________________________
____
____
____

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

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

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

Customer Initial Contact

Service is established

Needs Assessment continued

Monitoring an Existing Record

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

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

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

____
____
____
____

Describe your process for verifying validating the following:

Check by phone____

Credit Card Number____

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

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

____

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

____
____
____
____

What safeguards would you like to implement?

____
____
____
____

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

How do you authenticate transactions for existing Records?

Request

Request Fulfilled

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

External Cloud Policies

When the City of Columbia purchases services from an external cloud provider, as defined in this cloud strategy, the following policies must be followed:

2.0 Responsibilities of the City of Columbia

The City of Columbia will carry out the following tasks for every external cloud deployment as defined in this cloud strategy

2.1 The City of Columbia will establish a written agreement with the cloud vendor. This agreement will explicitly state the responsibilities of the vendor.
2.2 Prior to deployment, the City of Columbia will identify the regulations and standards that in force over the data or systems that may be moved to an external cloud. The City of Columbia will develop procedures and agreements with the cloud vendors to ensure compliance with all applicable regulations and standards.
2.3 The City of Columbia will establish an acceptable time frame for the vendor to respond to open records requests
2.4 The City of Columbia will establish a plan for the lifecycle of the service. The plan for the end of the service shall include what data will be extracted from the service, how data will be delivered, how the vendor will destroy data, and the price for these services. Data extracted from any system shall include transactional metadata, such as when data was added or changed and by whom.
2.5 The City of Columbia will calculate the anticipated load that will be placed on the City of Columbia internet connection. If the internet connection cannot handle the load a load management plan will be created and implemented prior to service implementation.
2.6 The City of Columbia will establish a business continuity plan that can be put into effect if the service ever becomes unavailable.
2.7 The City of Columbia shall manage all user accounts for the service. User accounts shall be managed through the existing security track procedures.

3.0 Responsibilities of the Vendors

All external cloud vendors, defined as vendors providing any cloud services as defined in this strategy to the City of Columbia must adhere to the following policies

3.1 Records Requests

3.1.1 The vendor will respond to records request within the timeframe stated in the agreement. The vendor will accept liability if the records request is not fulfilled in the agreed upon timeframe.

3.2 Using City of Columbia Domain Names

3.2.1 All cloud deployments that are intended to perform a service for our customers will be deployed using the gocolumbiamo.com domain name.

3.2.2 The City of Columbia IT Department will be the sole entity responsible for the gocolumbiamo.com domain name. The cloud vendor shall not expect to maintain DNS records belonging to the City of Columbia

3.2.2.1 The cloud vendor will provide the IP addresses used for the service prior to deployment. The City of Columbia IT Department will update the gocolumbiamo.com domain records accordingly.

3.2.2.2 The cloud vendor shall not change the addresses used with a frequency of greater than once per year

3.2.2.3 The cloud vendor shall notify the City of Columbia IT department in writing on official letterhead 30 days in advance of any IP address changes

3.2.2.4 The cloud vendor will use the gocolumbiamo.com only for the business purposes authorized by this agreement

3.2.3 Email from gocolumbiamo.com

When sending email from the service using the gocolumbiamo.com domain name, the following additional policies will be in effect

3.2.3.1 The cloud vendor will provide the IP addresses from which email will be sent. The City of Columbia IT Department will use this information to update the gocolumbiamo.com SPF record.

3.2.3.2 The addresses provided to the City of Columbia as required in 3.2.3.1 shall be only those IP addresses that are used to send email using the gocolumbiamo.com domain name.

3.2.3.3 The City of Columbia will update the gocolumbiamo.com SPF records according to the same policies and timelines as defined in 3.2.2 of this policy.

3.2.3.4 The cloud vendor will take all reasonable precautions to ensure that SPAM is not sent using the gocolumbiamo.com domain or from any IP address under cloud vendor control that has been associated with the gocolumbiamo.com domain.

3.2.3.5 The cloud vendor will react to email abuse reports in a timely manner

3.3 Standards and Regulations

3.3.1 The cloud vendor will adhere to relevant standards. For example, SaaS vendors deploying products over the web shall adhere to OWASP or similar standards.

3.3.2 The cloud vendor shall take responsibility for all regulatory compliance.

3.3.3 The cloud vendor shall conduct regular security audits of their systems. The security audits shall include internal and external review of system security and the security of all code used by the vendor. The vendor shall react promptly to mitigate the vulnerabilities identified by security audits.

3.4 System Integration

When an external cloud deployment requires access to existing information system infrastructure the following policies must be followed

3.4.1 Software should run with least possible privilege. For example, if database access needs to be given, the system account should have the least possible privilege; it should not run as a user that has access to schema outside of its need.

3.4.2 System account names should not be easily guessed. Passwords for these accounts should not be easily guessed and should be different from other customers with the same product. Connections from system accounts should be, where appropriate and possible, controlled via access lists.

3.5 Deployment and Customization

3.5.1 The cloud vendor shall disclose any authentication information that exists by default. The cloud vendor shall work with the City of Columbia to remove or change these accounts from their default values. The vendor shall not deploy services to the City of Columbia where system accounts are shared with other entities.

3.6 Encryption

3.6.1 Cloud vendor shall establish a suitable data encryption scheme for data in transit between the City of Columbia, its customers, and the vendor. The City of Columbia will determine the suitability of the encryption scheme.

3.6.2 Cloud vendor shall establish a suitable encryption for City of Columbia data while in storage for both live and backup media. The City of Columbia will determine the suitability of the encryption scheme.

3.6.3 No encryption scheme will be considered suitable if City of Columbia data can be recovered using the same decryption key as that of another customer of the cloud vendor.

3.7 Incident Preparation

3.7.1 The cloud vendor will take responsibility for keeping their system software up to date. Vendors should monitor relevant discussion boards and mailing lists for security problems with products they use.

3.7.2 The cloud vendors shall have a method for customers and others to report security problems. This method should be well publicized and accessible. Vendors should have a method for prioritizing and acting on reports of security problems.

3.7.3 The cloud vendors shall have a method for correcting discovered vulnerabilities. Vulnerabilities should be prioritized and corrected based on the risk vulnerability exploitation would pose to its customers. Vulnerability mitigation efforts should be tested by the vendor, as appropriate, prior to their release.

3.8 Incident Response

3.8.1 The cloud vendor will take responsibility for security incident handling if their system is compromised.

3.8.2 The cloud vendor shall immediately notify the City of Columbia of any breaches and will advise what information has been compromised. If this information is later found to be inaccurate the cloud vendor will immediately notify the City of Columbia with the correct information.

3.8.3 If investigation, containment, and eradication efforts by the City of Columbia incur costs while fault lies with the cloud vendor, the cloud vendor will assume the costs.

3.8.4 The cloud vendor will provide a rapid contact method for reporting suspected abuse, 24x7x365. The cloud vendor will react in a timely manner to abuse reports from the City of Columbia

3.8.5 The cloud vendor will provide their incident response plans. Response plans will include procedures for both security incident and disaster incident response.