AGREEMENT FOR THE PERFORMANCE OF SERVICES BY AND BETWEEN THE CITY OF SANTA CLARA, CALIFORNIA, AND ACCELA, INC.

PREAMBLE

This agreement for the performance of services ("Agreement") is by and between Accela, Inc., a California corporation, with its principal place of business located at 2633 Camino Ramon, Suite 500, San Ramon, CA 94853 ("Contractor"), and the City of Santa Clara, California, a chartered California municipal corporation with its primary business address at 1500 Warburton Avenue, Santa Clara, California 95050 ("City"). City and Contractor may be referred to individually as a "Party" or collectively as the "Parties" or the "Parties to this Agreement."

RECITALS

A. City desires to secure professional services more fully described in this Agreement, at Exhibit A, entitled "Scope of Services"; and

B. Contractor represents that it, and its subcontractors, if any, have the professional qualifications, expertise, necessary licenses and desire to provide certain goods and/or required services of the quality and type which meet objectives and requirements of City; and,

C. The Parties have specified herein the terms and conditions under which such services will be provided and paid for.

The Parties agree as follows:

AGREEMENT PROVISIONS

1. EMPLOYMENT OF CONTRACTOR.

City hereby employs Contractor to perform services set forth in this Agreement. To accomplish that end, City may assign a Project Manager to personally direct the Services to be provided by Contractor and will notify Contractor in writing of City's choice. City shall pay for all such materials and services provided which are consistent with the terms of this Agreement.

2. SERVICES TO BE PROVIDED.

Except as specified in this Agreement, Contractor shall furnish all technical and professional services for hosted subscriptions services, (collectively referred to as "Subscribed Services" as defined in Exhibit H, Paragraph 3) to satisfactorily complete the work required by City at his/her own risk and expense. Subscribed Services to be provided to City are more fully described in Exhibit H. All of the exhibits referenced in this Agreement are attached and are incorporated by this reference.

3. COMMENCEMENT OF SUBSCRIBED SERVICES.

CUSTOMER'S SUBSCRIPTION TERM COMMENCES ON A MUTUALLY AGREED UPON DATE TO OCCUR BEFORE SEPTEMBER 30, 2018 AND SAID DATE IS CUSTOMER'S "SERVICE DATE" FOR PURPOSES OF DESIGNATING THE START OF ANY SUBSCRIPTION TERM. FOR THE AVOIDANCE OF DOUBT, THE SERVICE DATE AND THE EFFECTIVE DATE MAY NOT BE THE SAME.

Contractor shall begin providing the Subscription services under the requirements of this Agreement upon receipt of written Notice to Proceed from City. Such notice shall be deemed to have occurred three (3) calendar days after it has been deposited in the regular United States mail. Contractor shall complete the Services within the time limits set forth in the Scope of Services or as mutually determined in writing by the Parties Contract execution.

When City determines that Contractor has satisfactorily completed the Services. Upon receipt of such notice, Contractor shall not incur any further costs under this Agreement. Contractor may request this determination of completion be made when, in its opinion, the Services have been satisfactorily completed.

4. QUALIFICATIONS OF CONTRACTOR - STANDARD OF WORKMANSHIP.

Contractor represents and maintains that it has the necessary expertise in the professional calling necessary to perform services, and its duties and obligations, expressed and implied, contained herein, and City expressly relies upon Contractor's representations regarding its skills and knowledge. Contractor shall perform such services and duties in conformance to and consistent with the professional standards of a specialist in the same discipline in the State of California.

The plans, designs, specifications, estimates, calculations, reports and other documents furnished under Exhibit A shall be of a quality acceptable to City. The criteria for acceptance of the work provided under this Agreement shall be a product of neat appearance, well organized, that is technically and grammatically correct, checked and having the maker and checker identified. The minimum standard of appearance, organization and content of the drawings shall be that used by City for similar projects.

5. TERM OF AGREEMENT.

Unless otherwise set forth in this Agreement or unless this paragraph is subsequently modified by a written amendment to this Agreement, the term of this Agreement shall begin on the Effective Date of this Agreement and terminate five (5) years from the Service Date. The Agreement may be renewed by the City, at its sole discretion, for two additional one (1) year terms.

6. MONITORING OF SUBSCRIBED SERVICES.

City may monitor the Subscribed Services performed under this Agreement to determine whether Contractor's operation conforms to City policy and to the terms of this Agreement. City may also monitor the Subscribed Services to be performed to determine whether financial operations are conducted in accord with applicable City, county, state, and federal requirements. If any action of Contractor constitutes a breach, City may terminate this Agreement pursuant to the provisions described herein.

7. PERFORMANCE OF SUBSCRIBED SERVICES.

Contractor shall perform all requested services in an efficient and expeditious manner and shall work closely with and be guided by City. Contractor shall be as fully responsible to City for the acts and omissions of its subcontractors, and of persons either directly or indirectly employed by them, as Contractor is for the acts and omissions of persons directly employed by it. Contractor will perform all Subscribed Services in a safe manner and in accordance with all federal, state and local operation and safety regulations.

8. BUSINESS TAX LICENSE REQUIRED.

Contractor must comply with Santa Clara City Code section 3.40.060, as that section may be amended from time to time or renumbered, which requires that any person who transacts or carries on any business in the City of Santa Clara pay business license tax to the City. A business tax certificate may be obtained by completing the Business Tax Affidavit Form and paying the applicable fee at the Santa Clara City Hall Municipal Services Division.

9. RESPONSIBILITY OF CONTRACTOR.

Contractor shall be responsible for the professional quality, technical accuracy and coordination of the Subscribed Services furnished by it, as set forth under this Agreement, including any exhibits or attachments. Neither City's review, acceptance, nor payments for any of the Services required under this Agreement shall be construed to operate as a waiver of any rights under this Agreement or of any cause of action arising out of the performance of this Agreement and Contractor shall be and remain liable to City (subject to any limitations in this Agreement) in accordance with applicable law for all damages to City caused by Contractor's Agreement, applicable federal, state, county, and/or municipal laws, ordinances, regulations, rules and orders.

10. COMPENSATION AND PAYMENT.

In consideration for Contractor's complete performance of Subscribed Services, City shall pay Contractor for all materials provided and services rendered by Contractor at the rate per hour for labor and cost per unit for materials as outlined in Exhibit B, entitled "SCHEDULE OF FEES."

Contractor will bill City on a monthly basis for Subscribed Services provided by Contractor during the preceding month, subject to verification by City. City will pay Contractor within thirty (30) days of City's receipt of invoice.

11. TERMINATION OF AGREEMENT.

Either Party may terminate this Agreement without cause by giving the other Party written notice ("Notice of Termination") which clearly expresses that Party's intent to terminate the Agreement, which will be effective on the following anniversary of the Subscription Term provided such Notice of Termination is received 30 days prior to the anniversary of the Effective Date of the upcoming Subscription Term. Notice of Termination shall become effective no less than thirty (30) calendar days after a Party receives such notice. After either Party terminates the Agreement, Contractor shall discontinue further services as of the effective date of termination, and City shall pay Contractor for all Subscribed Services satisfactorily performed up to such date.

If City renews the Agreement for additional one year terms after first five (5) year term, then upon such renewal either Party may terminate the Agreement without cause by giving the other Party Notice of Termination. Such Notice of Termination shall be effective ninety (90) days after receipt by the other Party. Upon any such Notice of Termination after the first five (5) year term, Contractor will refund any prepaid subscription fees covering the remainder of the subscription term after the effective date of termination.

Either party may terminate this Agreement if either Party materially breaches any terms and conditions of this Agreement after receiving a written notice describing the circumstances of the material breach, and the Party fails to correct the breach within thirty (30) calendar days. Upon any termination for cause by City, Contractor will refund any prepaid subscription fees covering the remainder of the subscription term after the effective date of termination.

12. NO ASSIGNMENT OR SUBCONTRACTING OF AGREEMENT.

City and Contractor bind themselves, their successors and assigns to all covenants of this Agreement. This Agreement shall not be assigned or transferred without the prior written approval of City. Contractor shall not hire subcontractors without express written permission from City.

13. NO THIRD PARTY BENEFICIARY.

This Agreement shall not be construed to be an agreement for the benefit of any third party or parties and no third party or parties shall have any claim or right of action under this Agreement for any cause whatsoever.

14. INDEPENDENT CONTRACTOR.

Contractor and all person(s) employed by or contracted with Contractor to furnish labor and/or materials under this Agreement are independent contractors and do not act as agent(s) or employee(s) of City. Contractor has full rights, however, to manage its employees in their performance of Subscribed Services under this Agreement. Contractor is not authorized to bind City to any contracts or other obligations.

15. NO PLEDGING OF CITY'S CREDIT.

Under no circumstances shall Contractor have the authority or power to pledge the credit of City or incur any obligation in the name of City. Contractor shall save and hold harmless the City, its City Council, its officers, employees, boards and commissions for expenses arising out of any unauthorized pledges of City's credit by Contractor under this Agreement.

16. CONFIDENTIALITY OF MATERIAL.

All ideas, memoranda, specifications, plans, manufacturing procedures, data, drawings, descriptions, documents, discussions or other information developed or received by or for Contractor and all other written information submitted to Contractor in connection with the performance of this Agreement shall be held confidential by Contractor and shall not, without the prior written consent of City, be used for any purposes other than the performance of the Subscribed Services nor be disclosed to an entity not connected with performance of the Subscribed Services. Nothing furnished to Contractor which is otherwise known to Contractor or becomes generally known to the related industry shall be deemed confidential.

17. USE OF CITY NAME OR EMBLEM.

Contractor shall not use City's name, insignia, or emblem, or distribute any information related to services under this Agreement in any magazine, trade paper, newspaper or other medium without express written consent of City.

18. OWNERSHIP OF MATERIAL.

Please refer to Exhibit H.

19. RIGHT OF CITY TO INSPECT RECORDS OF CONTRACTOR.

City, through its authorized employees, representatives or agents shall have the right during the term of this Agreement and for two (2) years from the date of final payment for goods or services provided under this Agreement, to audit the books and records of Contractor for the purpose of verifying any and all charges made by Contractor in connection with Contractor compensation under this Agreement, including termination of Contractor. Contractor agrees to maintain sufficient books and records in accordance with generally accepted accounting principles to establish the correctness of all charges submitted to City. Any expenses not so recorded shall be disallowed by City.

Contractor shall submit to City any and all reports concerning its performance under this Agreement that may be requested by City in writing. Contractor agrees to assist City in meeting City's reporting requirements to the State and other agencies with respect to Contractor's Subscribed Services hereunder.

20. CORRECTION OF SUBSCRIBED SERVICES.

Contractor agrees to correct any incomplete, inaccurate or defective Subscribed Services at no further costs to City, when such defects are due to the negligence, errors or omissions of Contractor.

21. FAIR EMPLOYMENT.

Contractor shall not discriminate against any employee or applicant for employment because of race, color, creed, national origin, gender, sexual orientation, age, disability, religion, ethnic background, or marital status, in violation of state or federal law.

22. HOLD HARMLESS/INDEMNIFICATION. PLEASE REFER TO EXHIBIT H.

23. INSURANCE REQUIREMENTS.

During the term of this Agreement, and for any time period set forth in Exhibit C, Contractor shall provide and maintain in full force and effect, at no cost to City insurance policies with respect to employees and vehicles assigned to the Performance of Subscribed Services under this Agreement with coverage amounts, required endorsements, certificates of insurance, and coverage verifications as defined in Exhibit C.

24. AMENDMENTS.

This Agreement may be amended only with the written consent of both Parties.

25. INTEGRATED DOCUMENT.

This Agreement represents the entire agreement between City and Contractor. No other understanding, agreements, conversations, or otherwise, with any representative of City prior to execution of this Agreement shall affect or modify any of the terms or obligations of this Agreement. Any verbal agreement shall be considered unofficial information and is not binding upon City.

26. SEVERABILITY CLAUSE.

In case any one or more of the provisions in this Agreement shall, for any reason, be held invalid, illegal or unenforceable in any respect, it shall not affect the validity of the other provisions, which shall remain in full force and effect.

27. WAIVER.

Contractor agrees that waiver by City of any one or more of the conditions of performance under this Agreement shall not be construed as waiver(s) of any other condition of performance under this Agreement.

28. NOTICES.

All notices to the Parties shall, unless otherwise requested in writing, be sent to City addressed as follows:

City of Santa Clara
Attention: Community Development Department, Building Division
1500 Warburton Avenue
Santa Clara, California 95050
or by facsimile at (408) 241-3823

And to Contractor addressed as follows:

Name: General Counsel
Address: 2633 Camino Ramon
San Ramon, CA94853
or by facsimile at 925-659-3201

If notice is sent via facsimile, a signed, hard copy of the material shall also be mailed. The workday the facsimile was sent shall control the date notice was deemed given if there is a facsimile machine generated document on the date of transmission. A facsimile transmitted after 1:00 p.m. on a Friday shall be deemed to have been transmitted on the following Monday.

29. CAPTIONS.

The captions of the various sections, paragraphs and subparagraphs of this Agreement are for convenience only and shall not be considered or referred to in resolving questions of interpretation.

30. LAW GOVERNING CONTRACT AND VENUE.

This Agreement shall be governed and construed in accordance with the statutes and laws of the State of California. The venue of any suit filed by either Party shall be vested in the state courts of the County of Santa Clara, or if appropriate, in the United States District Court, Northern District of California, San Jose, California.

31. DISPUTE RESOLUTION.

A. Unless otherwise mutually agreed to by the Parties, any controversies between Contractor and City regarding the construction or application of this Agreement, and claims arising out of this Agreement or its breach, shall be submitted to mediation within thirty (30) days of the written request of one Party after the service of that request on the other Party.

B. The Parties may agree on one mediator. If they cannot agree on one mediator, the Party demanding mediation shall request the Superior Court of Santa Clara County to appoint a mediator. The mediation meeting shall not exceed one day (eight (8) hours). The Parties may agree to extend the time allowed for mediation under this Agreement.

C. The costs of mediation shall be borne by the Parties equally.

D. For any contract dispute, mediation under this section is a condition precedent to filing an action in any court. In the event of mediation which arises out of any dispute related to this Agreement, the Parties shall each pay their respective attorney's fees, expert witness costs and cost of suit through mediation only. If mediation does not resolve the dispute, the Parties agree that the matter shall be litigated in a court of law, and not subject to the arbitration provisions of the Public Contracts Code.

32. COMPLIANCE WITH ETHICAL STANDARDS.

Contractor shall:

A. Read Exhibit D, entitled "ETHICAL STANDARDS FOR CONTRACTORS SEEKING TO ENTER INTO AN AGREEMENT WITH THE CITY OF SANTA CLARA, CALIFORNIA"; and,

B. Execute Exhibit E, entitled "AFFIDAVIT OF COMPLIANCE WITH ETHICAL STANDARDS."

33. AFFORDABLE CARE ACT OBLIGATIONS

To the extent Contractor is obligated to provide health insurance coverage to its employees pursuant to the Affordable Care Act ("Act") and/or any other similar federal or state law, Contractor warrants that it is meeting its obligations under the Act and will fully indemnify and hold harmless City for any penalties, fines, adverse rulings, or tax payments associated with Contractor's responsibilities under the Act.

34. CONFLICT OF INTERESTS.

This Agreement does not prevent either Party from entering into similar agreements with other parties. To prevent a conflict of interest, Contractor certifies that to the best of its knowledge, no City officer, employee or authorized representative has any financial interest in the business of Contractor and that no person associated with Contractor has any interest, direct or indirect, which could conflict with the faithful performance of this Agreement. Contractor is familiar with the provisions of California Government Code Section 87100 and following, and certifies that it does not know of any facts which would violate these code provisions. Contractor will advise City if a conflict arises.

CITY OF SANTA CLARA, CALIFORNIA
a chartered California municipal corporation

APPROVED AS TO FORM:

BRIAN DOYLE
City Attorney

Dated: 8/24/2018

DEANNA J. SANTANA
City Manager
1500 Warburton Avenue
Santa Clara, CA 95050
Telephone: (408) 615-2210
Fax: (408) 241-6771

ATTEST:

JENNIFER YAMAGUMA
Acting City Clerk

"CITY"

ACCELA, INC.
a California corporation

Dated: May 29, 2018

By: _____
(Signature of Person executing the Agreement on behalf of Contractor)

Name: Jonathon Knight

Title: Chief Customer Officer

Local Address: 2633 Camino Ramon, Suite 500
San Ramon, CA 94583

Email Address: jknight@accela.com

Telephone: (925) 359-3200

Fax: (925) 659-3201

"CONTRACTOR"

S:\Attorney\AGREEMENTS\Service\OVER $50K SERVICE AGREEMENT FORM.doc

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT A

SCOPE OF SUBSCRIBED SERVICES

This exhibit is not used in this agreement. For the software subscription terms and conditions, please refer to Exhibit H.

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT B

FEE SCHEDULE

In no event shall the amount billed to City by Contractor for services under this Agreement exceed One Million Two Hundred Eighteen Thousand Six Hundred Fifty-Nine Dollars and Ninety-Eight Cents ($1,218,659.98), subject to budget appropriations.

Citizen Access

PART #	PRODUCT NAME	QTY	NET PRICE
SS10AACAPOP0001	Accela Citizen Access - Subscription Population	125,948	USD 12,594.80
	Subtotal		USD 12,594.80

Civic Platform

PART #	PRODUCT NAME	QTY	NET PRICE
SS10APFMSLVR001	Accela Civic Platform Silver - Subscription User	40	USD 71,520.00
SS10APFMSLVR001	Accela Civic Platform Silver - Subscription User	140	USD 257,829.60
SS10APFMSLVR001	Accela Civic Platform Silver - Subscription User	140	USD 265,563.93
SS10APFMSLVR001	Accela Civic Platform Silver - Subscription User	140	USD 273,531.52
SS10APFMSLVR001	Accela Civic Platform Silver - Subscription User	140	USD 281,737.01
	Subtotal		USD 1,150,182.06

PART #	PRODUCT NAME	QTY	NET PRICE
SS10AACAPOP0001	Accela Citizen Access - Subscription Population	125,948	USD 13,363.08
SS10AACAPOP0001	Accela Citizen Access - Subscription Population	125,948	USD 13,753.52
SS10AACAPOP0001	Accela Citizen Access - Subscription Population	125,948	USD 14,169.15
SS10AACAPOP0001	Accela Citizen Access - Subscription Population	125,948	USD 14,597.37
	Subtotal		USD 55,883.12

TOTAL: USD 1,218,659.98

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT C

INSURANCE REQUIREMENTS

INSURANCE COVERAGE REQUIREMENTS

Without limiting the Contractor's indemnification of the City, and prior to commencing any of the Services required under this Agreement, the Contractor shall provide and maintain in full force and effect, at its sole cost and expense, the following insurance policies with at least the indicated coverages, provisions and endorsements:

A. COMMERCIAL GENERAL LIABILITY INSURANCE

1. Commercial General Liability Insurance policy which provides coverage at least as broad as policy limits, which are subject to review, but shall in no event be less than, the following:

   $1,000,000 Each Occurrence
   $2,000,000 General Aggregate
   $2,000,000 Products/Completed Operations Aggregate
   $1,000,000 Personal Injury

2. Exact structure and layering of the coverage shall be left to the discretion of Contractor; however, any excess or umbrella policies used to meet the required limits shall be at least as broad as the underlying coverage and shall otherwise follow form.

3. The following provisions shall apply to the General Commercial Liability policy as well as any umbrella policy maintained by the Contractor to comply with the insurance requirements of this Agreement:

   a. Coverage shall be on a "pay on behalf" basis with defense costs payable in addition to policy limits;

   b. There shall be no cross liability exclusion which precludes coverage for claims or suits by one insured against another; and

   c. Coverage shall apply separately to each insured against whom a claim is made or a suit is brought, except with respect to the limits of liability.

B. BUSINESS AUTOMOBILE LIABILITY INSURANCE

Business automobile liability insurance policy which provides coverage at least as broad as ISO form CA 00 01 with policy limits a minimum limit of not less than one million dollars ($1,000,000) each accident using, or providing coverage at least as broad as, Insurance Services Office form CA 00 01. Liability coverage shall apply to all non-owned and hired autos.

C. WORKERS' COMPENSATION

1. Workers' Compensation Insurance Policy as required by statute and employer's liability with limits of at least one million dollars ($1,000,000) policy limit Bodily Injury by disease, one million dollars ($1,000,000) each accident/Bodily Injury and one million dollars ($1,000,000) each employee Bodily Injury by disease.

2. The indemnification and hold harmless obligations of Contractor included in this Agreement shall not be limited in any way by any limitation on the amount or type of damage, compensation or benefit payable by or for Contractor or any subcontractor under any Workers' Compensation Act(s), Disability Benefits Act(s) or other employee benefits act(s).

3. This policy must include a Waiver of Subrogation in favor of the City of Santa Clara, its City Council, commissions, officers, employees, volunteers and agents.

D. COMPLIANCE WITH REQUIREMENTS

All of the following clauses and/or endorsements, or similar provisions, must be part of each commercial general liability policy.

1. Additional Insureds. The Commercial General Liability insurance will include the City of Santa Clara, its City Council, commissions, officers, employees, volunteers and agents are hereby added as additional insureds in respect to liability arising out of Contractor's work for City.

2. Primary and non-contributing. Commerical General Liability policy provided by Contractor shall contain language or be endorsed to contain wording making it primary insurance as respects to, and not requiring contribution from, any other insurance which the Indemnities may possess, including any self-insurance or self-insured retention they may have. Any other insurance Indemnities may possess shall be considered excess insurance only and shall not be called upon to contribute with Contractor's insurance.

3. Cancellation.

   a. Commercial General Liability policy shall contain language or be endorsed to reflect that no cancellation of the coverage provided due to non-payment of premiums shall be effective until written notice has been

given to City at least ten (10) days prior to the effective date of such cancellation

b. Each insurance policy shall contain language or be endorsed to reflect that no cancellation of the coverage provided for any cause save and except non-payment of premiums shall be effective until written notice has been given to City at least thirty (30) days prior to the effective date of such cancellation.

4. Other Endorsements. Other endorsements may be required for policies other than the commercial general liability policy if specified in the description of required insurance set forth in Sections A through D of this Exhibit C, above.

E. ADDITIONAL INSURANCE RELATED PROVISIONS

Contractor and City agree as follows:

1. Contractor agrees that upon request by City, all agreements with, and insurance compliance documents provided by, such subcontractors and others engaged in the project will be submitted to City for review.

2. Contractor agrees to be responsible for ensuring that no contract used by any party involved in any way with the project reserves the right to charge City or Contractor for the cost of additional insurance coverage required by this Agreement. Any such provisions are to be deleted with reference to City. It is not the intent of City to reimburse any third party for the cost of complying with these requirements. There shall be no recourse against City for payment of premiums or other amounts with respect thereto.

3. The City reserves the right to withhold payments from the Contractor in the event of material noncompliance with the insurance requirements set forth in this Agreement.

F. EVIDENCE OF COVERAGE

Prior to commencement of any Services under this Agreement, Contractor, and shall, at its sole cost and expense, provide and maintain not less than the minimum insurance coverage with the endorsements and deductibles indicated in this Agreement. Such insurance coverage shall be maintained with insurers, and under forms of policies, satisfactory to City and as described in this Agreement. Contractor shall file with the City all certificates and endorsements for the required insurance policies for City's approval as to adequacy of the insurance protection.

G. EVIDENCE OF COMPLIANCE

Contractor or its insurance broker shall provide the required proof of insurance compliance, consisting of Insurance Services Office (ISO) endorsement forms or their equivalent and the ACORD form 25-S certificate of insurance (or its equivalent),

evidencing all required coverage shall be delivered to City, or its representative as set forth below, at or prior to execution of this Agreement. Upon City's request Contractor shall submit to City copies of portions of the actual insurance policies or renewals or replacements to the extent necessary to ensure compliance with this Exhibit C. Unless otherwise required by the terms of this Agreement, all certificates, endorsements, coverage verifications and other items required to be delivered to City pursuant to this Agreement shall be mailed to:

EBIX Inc.
City of Santa Clara, Community Development Department, Building Division
P.O. Box 100085 – S2 or 1 Ebix Way
Duluth, GA 30096 John's Creek, GA 30097

Telephone number: 951-766-2280
Fax number: 770-325-0409
Email address: ctsantaclara@ebix.com

H. QUALIFYING INSURERS

All of the insurance companies providing insurance for Contractor shall have, and provide written proof of, an A. M. Best rating of at least A minus 6 (A- VI) or shall be an insurance company of equal financial stability that is approved by the City or its insurance compliance representatives.

S:\Attorney\INSURANCE\CITY\EXHIBIT C-02 Contract over $50,000 limited exposure.doc

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCLA, INC.

EXHIBIT D

ETHICAL STANDARDS FOR CONTRACTORS SEEKING TO ENTER INTO AN AGREEMENT WITH THE CITY OF SANTA CLARA, CALIFORNIA

Termination of Agreement for Certain Acts.

A. The City may, at its sole discretion, terminate this Agreement in the event any one or more of the following occurs:

1. If a Contractor[1] does any of the following:

   a. Is convicted[2] of operating a business in violation of any Federal, State or local law or regulation;

   b. Is convicted of a crime punishable as a felony involving dishonesty[3];

   c. Is convicted of an offense involving dishonesty or is convicted of fraud or a criminal offense in connection with: (1) obtaining; (2) attempting to obtain; or, (3) performing a public contract or subcontract;

   d. Is convicted of any offense which indicates a lack of business integrity or business honesty which seriously and directly affects the present responsibility of a City contractor or subcontractor; and/or,

   e. Made (or makes) any false statement(s) or representation(s) with respect to this Agreement.

---

[1] For purposes of this Agreement, the word "Consultant" (whether a person or a legal entity) also refers to "Contractor" and means any of the following: an owner or co-owner of a sole proprietorship; a person who controls or who has the power to control a business entity; a general partner of a partnership; a principal in a joint venture; or a primary corporate stockholder [i.e., a person who owns more than ten percent (10%) of the outstanding stock of a corporation] and who is active in the day to day operations of that corporation.

[2] For purposes of this Agreement, the words "convicted" or "conviction" mean a judgment or conviction of a criminal offense by any court of competent jurisdiction, whether entered upon a verdict or a plea, and includes a conviction entered upon a plea of nolo contendere within the past five (5) years.

[3] As used herein, "dishonesty" includes, but is not limited to, embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, failure to pay tax obligations, receiving stolen property, collusion or conspiracy.

2. If fraudulent, criminal or other seriously improper conduct of any officer, director, shareholder, partner, employee or other individual associated with the Contractor can be imputed to the Contractor when the conduct occurred in connection with the individual's performance of duties for or on behalf of the Contractor, with the Contractor's knowledge, approval or acquiescence, the Contractor's acceptance of the benefits derived from the conduct shall be evidence of such knowledge, approval or acquiescence.

B. The City may also terminate this Agreement in the event any one or more of the following occurs:

1. The City determines that Contractor no longer has the financial capability[4] or business experience[5] to perform the terms of, or operate under, this Agreement; or,

2. If City determines that the Contractor fails to submit information, or submits false information, which is required to perform or be awarded a contract with City, including, but not limited to, Contractor's failure to maintain a required State issued license, failure to obtain a City business license (if applicable) or failure to provide and maintain bonds and/or insurance policies required under this Agreement.

C. In the event a prospective Contractor (or bidder) is ruled ineligible (debarred) to participate in a contract award process or a contract is terminated pursuant to these provisions, Contractor may appeal the City's action to the City Council by filing a written request with the City Clerk within ten (10) days of the notice given by City to have the matter heard. The matter will be heard within thirty (30) days of the filing of the appeal request with the City Clerk. The Contractor will have the burden of proof on the appeal. The Contractor shall have the opportunity to present evidence, both oral and documentary, and argument.

---

[4] Contractor becomes insolvent, transfers assets in fraud of creditors, makes an assignment for the benefit of creditors, files a petition under any section or chapter of the federal Bankruptcy Code (11 U.S.C.), as amended, or under any similar law or statute of the United States or any state thereof, is adjudged bankrupt or insolvent in proceedings under such laws, or a receiver or trustee is appointed for all or substantially all of the assets of Contractor.

[5] Loss of personnel deemed essential by the City for the successful performance of the obligations of the Contractor to the City.

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT E

AFFIDAVIT OF COMPLIANCE WITH ETHICAL STANDARDS

I hereby state that I have read and understand the language, entitled "Ethical Standards" set forth in Exhibit D. I have the authority to make these representations on my own behalf or on behalf of the legal entity identified herein. I have examined appropriate business records, and I have made appropriate inquiry of those individuals potentially included within the definition of "Contractor" contained in Ethical Standards at footnote 1.

Based on my review of the appropriate documents and my good-faith review of the necessary inquiry responses, I hereby state that neither the business entity nor any individual(s) belonging to said "Contractor" category [i.e., owner or co-owner of a sole proprietorship, general partner, person who controls or has power to control a business entity, etc.] has been convicted of any one or more of the crimes identified in the Ethical Standards within the past five (5) years.

The above assertions are true and correct and are made under penalty of perjury under the laws of the State of California.

ACCELA, INC.

a California corporation

By: _____
Signature of Authorized Person or Representative

Name: Jonathon Knight

Title: Chief Customer Officer

NOTARY'S ACKNOWLEDGMENT TO BE ATTACHED

Please execute the affidavit and attach a notary public's acknowledgment of ~~execution of~~ the affidavit by the signatory. If the affidavit is on behalf of a corporation, partnership, ~~or other~~ legal entity, the entity's complete legal name and the title of the person signing on behalf of the legal entity shall appear above. Written evidence of the authority of the person executing this affidavit on behalf of a corporation, partnership, joint venture, or any other legal entity, other than a sole proprietorship, shall be attached.

See attached CA Acknowledgment

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT CIVIL CODE § 1189

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of Contra Costa }

On May 29th 2018 before me, Esther Sigona, Notary Public,
Date *Here Insert Name and Title of the Officer*

personally appeared Jonathan Knight
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

ESTHER SIGONA
Notary Public - California
Contra Costa County
Commission # 2237556
My Comm. Expires Apr 9, 2022

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature _____
Signature of Notary Public

Place Notary Seal and/or Stamp Above

OPTIONAL

Completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: _____

Document Date: _____ Number of Pages: _____

Signer(s) Other Than Named Above: _____

Capacity(ies) Claimed by Signer(s)

Signer's Name: _____	Signer's Name: _____
☐ Corporate Officer – Title(s): _____	☐ Corporate Officer – Title(s): _____
☐ Partner – ☐ Limited ☐ General	☐ Partner – ☐ Limited ☐ General
☐ Individual ☐ Attorney in Fact	☐ Individual ☐ Attorney in Fact
☐ Trustee ☐ Guardian of Conservator	☐ Trustee ☐ Guardian of Conservator
☐ Other: _____	☐ Other: _____
Signer is Representing: _____	Signer is Representing: _____

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT F

SPECIFICATIONS AND REQUIREMENTS

EXHIBIT F
SPECIFICATIONS AND REQUIREMENTS

Product Specifications

Accela's solution for the City's permitting and inspection functions will leverage Accela Civic Platform's Land Management solution along with its integral components for Citizen Access, GIS, and Mobile.

Land Management

The Civic Platform allows the City to automate and streamline your civic processes related to permitting.

Accela's Land Management makes it easy for state, county and city agencies of all sizes to coordinate activities for the consideration and approval of land use and building permits, inspections and enforcement to meet your jurisdiction codes. The solution saves time, increases productivity and connects government agencies to the businesses, professionals and citizens they serve.

Accela's Land Management:

- **Simplifies the permit process.** Manage your entire permitting process including application check-in, plan reviews, fee calculation and collection, inspections, sign-offs, task lists, and more. Easily manage both the proposed plan and the relationships to the project – including imposing restrictions on transactions, property or individuals until compliance measures and fees are satisfied.
- **Engages your citizens 24/7/365 days of the year.** Accela's Citizen Access and IVR capabilities provide quick and easy access to information about permits and inspections directly from any telephone, web browser, or mobile device.
- **Visualizes information with built-in GIS capabilities**, which deliver mapping and routing functionality to the enterprise. This overlays government data onto GIS maps and allows customers to initiate and manage permit activities from a geospatial platform.
- **Provides online access to save time for agency staff out in the field.** Productivity apps, such as Analytics, Inspector, and Contractor Central, connect and equip agency field workers with the right mobile device for the job.

User Interface

Accela's web-based Civic Platform user interface shows several screens on a single page and are configured to meet the needs of individual user roles.

Among the most frequently used screens are those presenting alerts and notifications, upcoming and overdue tasks, performance-based charting, and frequently used data queries. When used with Accela's GIS capabilities, government activity data is viewable on a map screen, confirming the solution's versatility in how data is represented.

When used with Accela's mobile capabilities, all land management activity data is available to field staff, enabling a full mobile field office solution. Inspector assignments, schedules, routes, status reports, and inspection results are all logically presented. Data collected in the field is recorded electronically and uploaded to the solution for immediate availability throughout the enterprise.

Further extending Land Management offerings to the public are Accela's Citizen Access, which promote true government transparency and citizen self-service by bringing government services to the public 24/7. Self-service options may include property information, online applications, fee collection and inspection scheduling. In eliminating the need for in-person and paper processing, these solution components unite governments and their constituents through accessible technology while reducing costs.

Citizen Access

Citizen participation and collaboration are now one of the most urgent needs facing our government. The ability to put processes online greatly assists this mission in two key ways — by allowing applicants to take advantage of self-service and by increasing agency staff productivity. Another obvious advantage is the solution's inherent ability to address budgetary concerns and help government do more with less.

Accela has long been cognizant of the need for transparency and accountability. Through a self-service web portal and an open user interface, Citizen Access extends government services to the public 24-hours a day by providing members of the public with online access to apply for land development applications, permits, licenses, schedule inspections, request services, and perform tasks from the convenience of their home, office or job site. This presents a useful way for public users to interact with your agency in an efficient manner.

By configuring a custom welcome page and designing page flows that are intuitive, easy-to-use, and come with agency defined context specific help agencies can better engage and connect with their public. This enables truly transparent government operations. Citizen Access supports IE 11 and the latest stable versions of Firefox, Safari, Chrome, and Opera browsers.

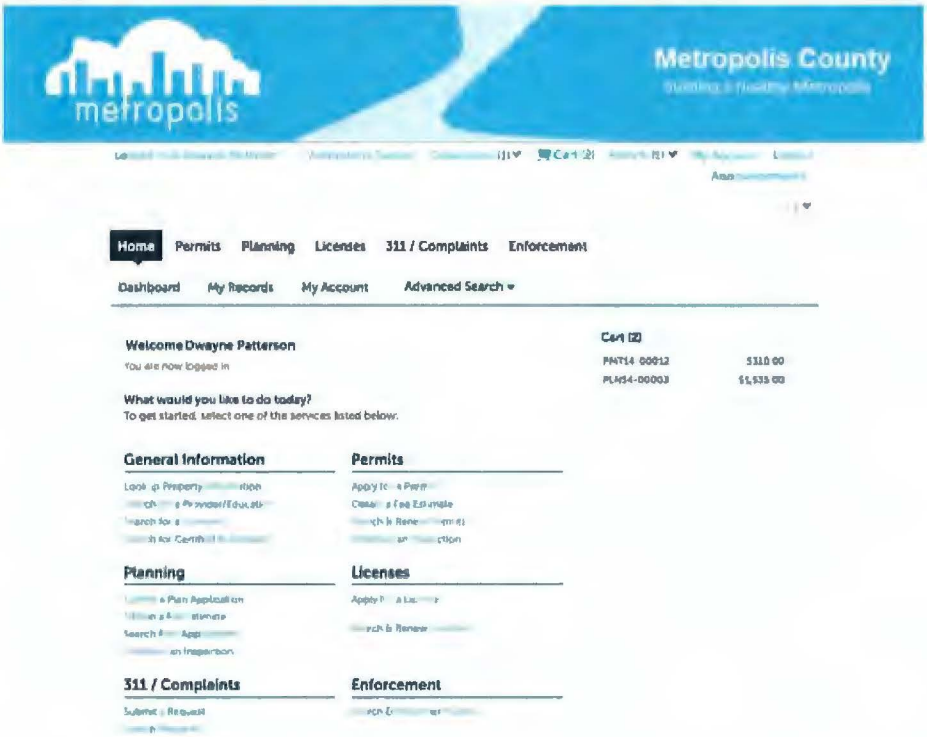


Exhibit 1: Citizen Access Dashboard

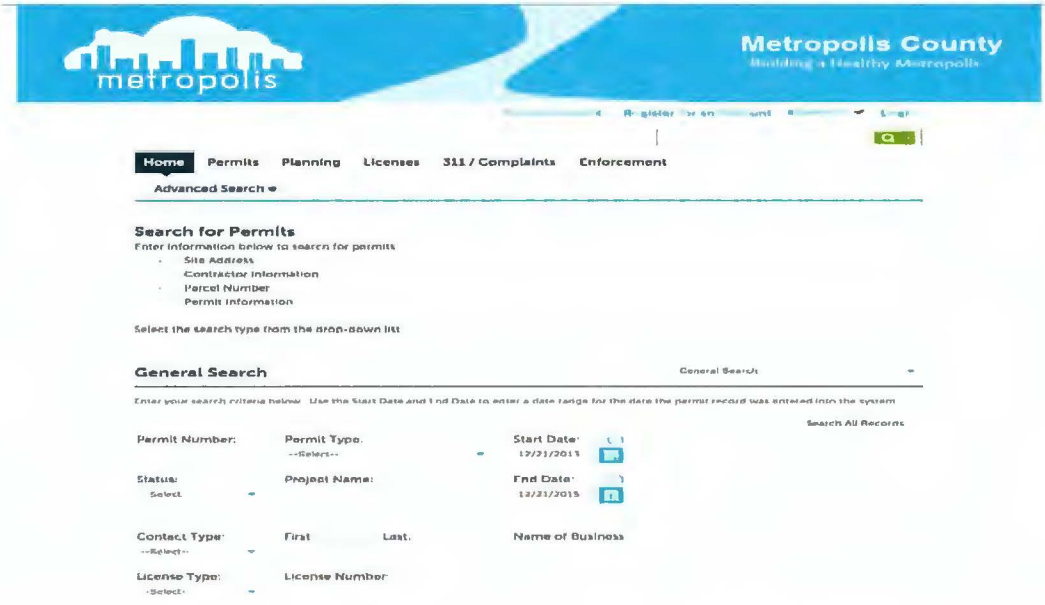


Exhibit 2: Advanced search in Citizen Access

Among the many citizen privileges available, external users can take advantage of the following capabilities:

- Apply for permits
- Research parcels using Esri GIS
- Submit complaints
- Submit requests for service
- Check status of applications, permits, and inspections
- Upload electronic plans and other documents or photographs
- View solution generated alerts and notifications
- View a history of all complaints/requests
- Conduct searches
- Pay fees
- View data on maps
- Search addresses/parcel information
- Access government documents
- View all parcel history

Citizen Access is available in English (U.S. and Australian), Spanish, French, Arabic, Chinese, Portuguese, and Vietnamese language packs. Additionally, we developed the solution so that all financial transactions are PCI DSS compliant. Furthermore, our solution is Section 508c compliant, to make our products accessible to people with disabilities — such as blindness and low vision.

Purchase of Citizen Access includes the mobile application, Mobile Citizen Access, which further enhances accessibility options for public users. Constituents now enjoy a truly mobile access to government data, using iOS or Android devices.

Citizen Access inherits the exact business rules established in Land Management. System administrators simply select which service request activities are to be made available to the public. Additionally, the Civic Platform utilizes one central database---data submitted through Citizen Access is immediately available for processing by back office users in Land Management.

.

GIS

The Civic Platform includes GIS functionality out of the box to help streamline mapping processes. The technology integration offers governments a geographic view of all land-use, zoning and infrastructure information associated with parcels, permits, inspections, and service requests, and works seamlessly with Esri maps, layering the information for increased visibility. The Civic Platform map component is built using the Esri JavaScript map control and consumes GIS services published from the agency's ArcGIS Server or ArcGIS Online, as well as can consume Open Geospatial Consortium Web Mapping and Web Feature Service map services.

GIS also provides visualization of an agency's government data geographically by plotting locations of activities captured in the Civic Platform on the map. GIS provides enhanced user experience with

- Optimal server response times
- Smooth panning
- Context-sensitive commands and menu items

- Drag and drop functionality
- Client side graphic rendering

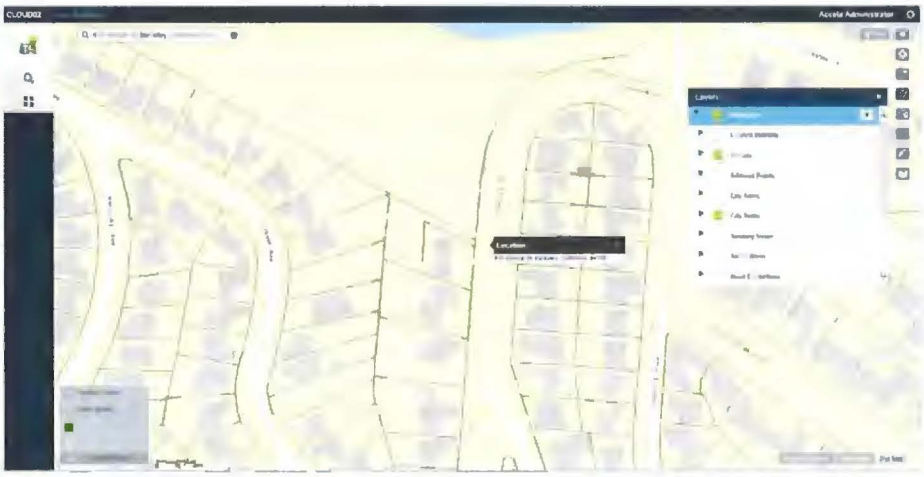
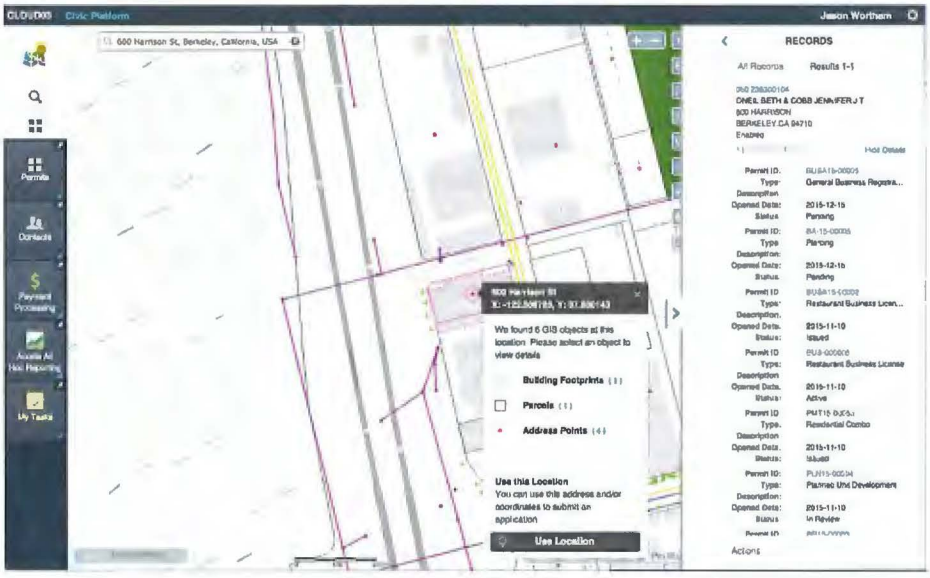


Exhibit 3: GIS Map Interface

Accela's GIS gives users the option to initiate and manage all land management activities from a map interface. GIS is a bi-directional interface enabling viewing, interaction, and presentation of both tabular and spatial information. It leverages an agency's GIS database and map services published by one or more ArcGIS Servers. Base maps published from one agency can be combined with map data from another agency to provide a comprehensive view of geographic information.



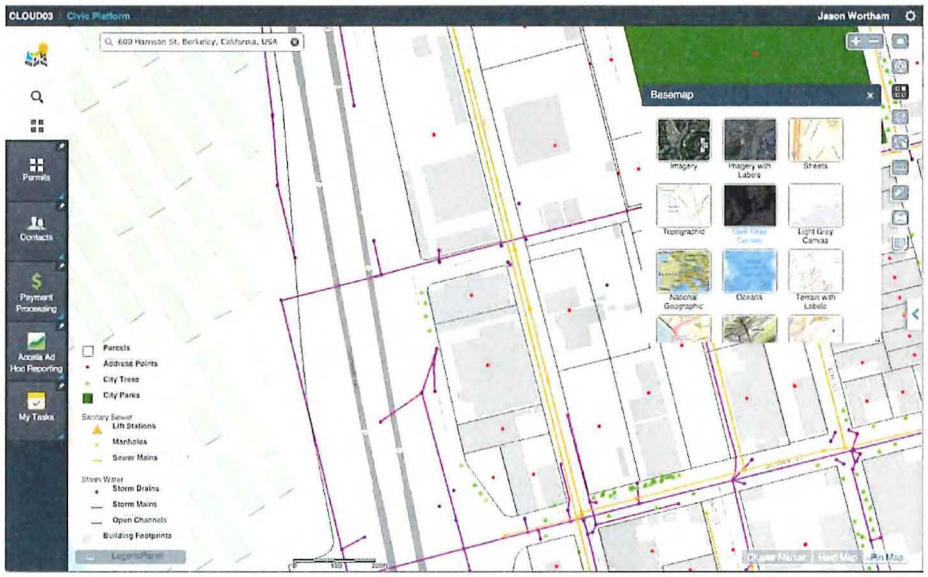


Exhibit 4: Share the Civic Platform data in Esri ArcGIS Online

Optional map editing tools empower end users to draw new features using points, lines, or polygons to represent actual geographic elements or assets. Once these new features are created, they can be associated with transactions in the Civic Platform database. GIS supports efficient fieldwork through its routing features. Inspection schedules can be automatically routed or users can choose to optimize inspection schedules based on shortest distance or travel time.

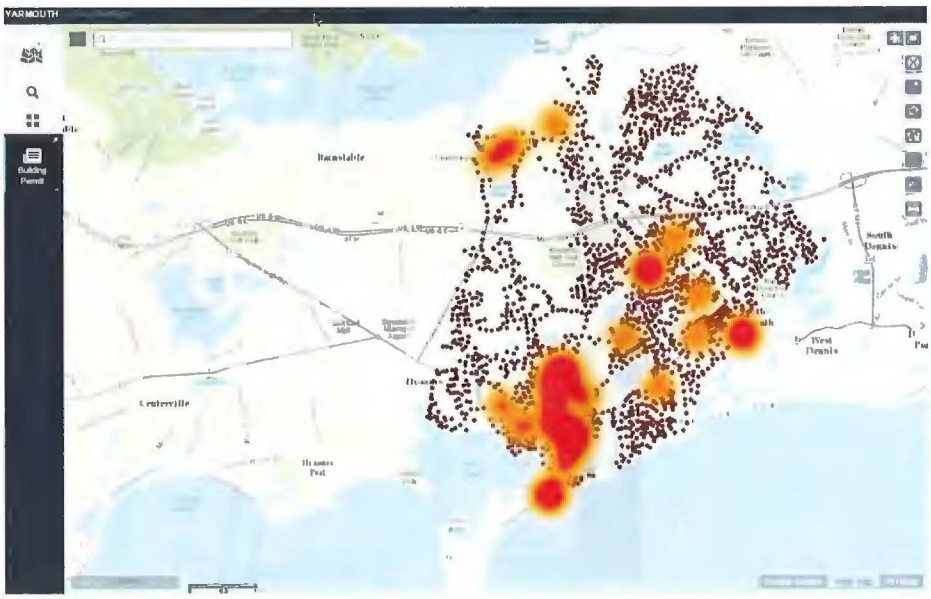


Exhibit 5: Accela GIS Heat Map

Customers may enhance user views by adding the agency's ArcGIS map layers to the map viewer. Together, these data sources, united with Accela transaction data, offer the most comprehensive visual representation of government and location data available. Users can manage, edit, and update data from the map viewer. The map viewer presents reference data and context-based action items for a selected parcel(s) (i.e., create a record, show record, create inspection, etc.).

When deployed with Mobile, routing capabilities are available whether connected or disconnected from the network. Routes and driving directions can be saved and printed as needed. Optimized routing can be done one of two ways:

1. To use an agency's street file, that agency needs ArcGIS Server Network Extension and a published routing service. The agency typically creates the network via ArcGIS Desktop and the Network Analyst extension.

2. The agency may not have a quality street file in an Esri GIS format or does not have the additional Esri software list noted above in number one.

The following is a list of features/functions that are available out of the box in Accela's GIS solution:

- Plotting event locations (address, parcel or asset matching)
- Start new application/transaction from selected map feature
- Navigation (pan, zoom in/out, zoom to scale/selected/full extent)
- Select (by line, polygon, rectangle)
- Buffer selection
- Attach/associate feature to transaction record
- Add selected features to a Set in Accela
- Redlining (point, line, polygon and text box)
- Identify (click on map and see attributes of features)
- Reverse geocoding for mobile mapping

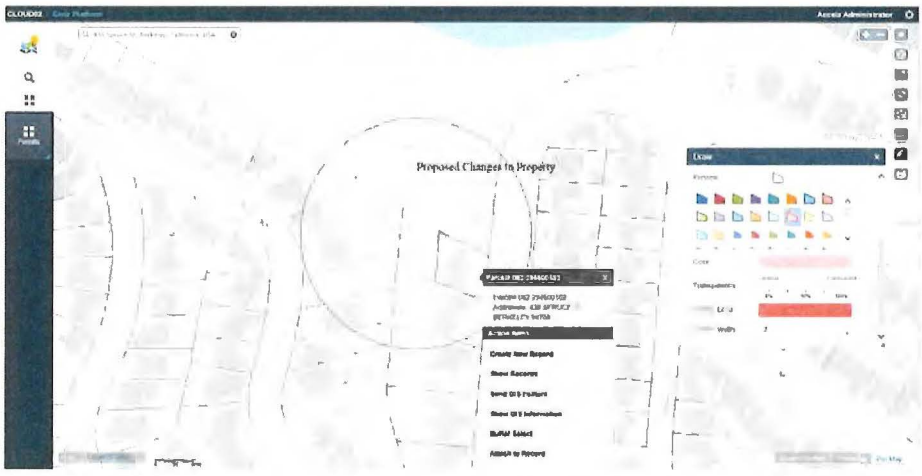


Exhibit 6: Redlining in Accela GIS

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT G

CLOUD SERVICE PROVIDER CHECKLIST

Title:

Date:

Compliance	Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Audit and Accountability (AU) security controls.
Compliance	Independent Audits	CO-02	CO-02.1	Do you allow (describe/explain/attach/embed associated documents) tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402/ISO27001:2005 or similar third party audit reports?	Yes. Accela makes the following reports available to clients and potentia clients with NDA's on file for their review: • SSAE 16/SOC 2 • PCI AOC • NIST 800-53 Controls Status and POAM summary for any remediation efforts that may be in progress at the time.
Compliance			CO-02.2	Do you conduct (describe/explain/attach/embed associated documents) network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes. Pentetration tests, that include assessing the infrastructure and application, are completed bi-annually. Vulenerability scans are completed monthly.
Compliance			CO-02.3	Do you conduct (describe/explain/attach/embed associated documents) regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?	Yes. Pentetration tests, that include assessing the infrastructure and application, are completed bi-annually. Vulenerability scans are completed monthly.
Compliance			CO-02.4	Do you conduct (describe/explain/attach/embed associated documents) internal audits regularly as prescribed by industry best practices and guidance?	Yes. External SSAE 16/SOC 2 and PCI audits are completed annualy. External NIST 800-53 audits are completed bi-annually. Accela has an internal audit function that is continuously reviewing compliance with specific control families.

Compliance			CO-02.5	Do you conduct (describe/explain/attach/embed associated documents) external audits regularly as prescribed by industry best practices and guidance?	Yes. External SSAE 16/SOC 2 and PCI audits are completed annualy. External NIST 800-53 audits are completed bi-annually. Accela has an internal audit function that is continuously reviewing compliance with specific control families.
Compliance			CO-02.6	Are the results of the network penetration tests available to tenants at their request?	No, due to the sensitive nature of this information. However, result summaries and remediation plans are available for client review.
Compliance			CO-02.7	Are the results of internal and external audits available to tenants at their request?	No, due to the sensitive nature of this information. However, result summaries and remediation plans are available for client review.
Compliance	Third Party Audits	CO-03	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?	No. Due to the instability this may cause in shared tenant environment, this activity is carefully planned and coordinated by Accela.
Compliance			CO-03.2	Do you have (describe/explain/attach/embed associated documents) external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes. Pentetration tests, that include assessing the infrastructure and application, are completed bi-annually. Vulenerability scans are completed monthly.
Compliance	Contact / Authority Maintenance	CO-04	CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes. Accela maintains contact with various parties associated with NIST 800-53, PCI-DSS and SSAE 16 compliance regulations.
Compliance	Information System Regulatory Mapping	CO-05	CO-05.1	Do you have (describe/explain/attach/embed associated documents) the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes. Tenants are logically segmented at the database attribute level.

			CO-05.2	Do you have (describe/explain/attach/embed associated documents) capability to logically segment and recover data for specific customer in the case of a failur or data loss?	Yes. Tenants are logically segmented at the database attribute level. Procedures are in place for tenant data restoration.
Compliance	Intellectual Property	CO-06	CO-06.1	Do you have (describe/explain/attach/embed associated documents) policies and procedures in place describing what controls you have in place to protect tenants intellectual property?	Yes. Accela has several policies that address confidentiality, integrity and availability of client data.
Compliance	Intellectual Property	CO-07	CO-07.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved?	Accela does not mine client data.
Compliance	Intellectual Property	CO-08	CO-08.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide (describe/explain/attach/embed associated documents) tenants the ability to opt-out?	Accela does not mine client data.
Data Governance					
Data Governance	Ownership / Stewardship	DG-01	DG-01.1	Do you follow (describe/explain/attach/embed associated documents) a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Media Protection (MP) security controls.

Data Governance	Classification	DG-02	DG-02.1	Do you provide (describe/explain/attach/embed associated documents) a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)?	No, however, platform instantiation is carefully managed and monitored.
Data Governance			DG-02.2	Do you provide (describe/explain/attach/embed associated documents) a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)?	Yes. All hardware is tracked as part of asset management.
Data Governance			DG-02.3	Do you have (describe/explain/attach/embed associated documents) a capability to use system geographic location as an authentication factor?	No.
Data Governance			DG-02.4	Can you provide (describe/explain/attach/embed associated documents) the physical location/geography of storage of a tenant's data upon request?	Yes. All data is housed in the continental United States in either our East or West Coast data centers.
Data Governance			DG-02.5	Do you allow (describe/explain/attach/embed associated documents) tenants to define acceptable geographical locations for data routing or resource instantiation?	No. Accela carefully selects georgraphical locations for services and data based on numerous factors, including throughputassociated with physical distance and client load patterns.
Data Governance	Handling / Labeling / Security Policy	DG-03	DG-03.1	Are Policies and procedures established for labeling, handling and security of data and objects, which contain data?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Media Protection (MP) security controls.

Data Governance			DG-03.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Applications do not use data labeling. Although Public or private/sensitive data are implied during system implementation/configuration, it is which controlled by access rights. At the application level, 'sensitive data' is managed by leveraging hashing & encryption algorithms. No labeling is used at the database level.
Data Governance	Retention Policy	DG-04	DG-04.1	Do you have (describe/explain/attach/embed associated documents) technical control capabilities to enforce tenant data retention policies?	Accela does not delete or archive client data. Clients have the capability, via the user interface or a special Services request, to delete and archive data.
Data Governance			DG-04.2	Do you have (describe/explain/attach/embed associated documents) a documented procedure for responding to requests for tenant data from governments or third parties?	Yes. Accela does not grant requests for client data from 3rd parties or governments unless required by written subpoena.
Data Governance	Secure Disposal	DG-05	DG-05.1	Do you support (describe/explain/attach/embed associated documents) secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the tenant?	Data is deleted but no extra steps to wipe slack space are taken. That data is reclaimed and used by other DB segments as part of normal processing.
Data Governance			DG-05.2	Can you provide (describe/explain/attach/embed associated documents) a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Data is deleted but no extra steps to wipe slack space are taken. That data is reclaimed and used by other DB segments as part of normal processing.

Data Governance	Nonproduction Data	DG-06	DG-06.1	Do you have (describe/explain/attach/embed associated documents) procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes. Accela has policies in place prohibiting the exporting of production data to non-production environments with the exception of using sanitized production data for testing and troubleshooting purposes.
Data Governance	Information Leakage	DG-07	DG-07.1	Do you have (describe/explain/attach/embed associated documents) controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment?	Yes.
Data Governance			DG-07.2	Do you have (describe/explain/attach/embed associated documents) a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?	Yes.
Data Governance	Risk Assessments	DG-08	DG-08.1	Do you provide (describe/explain/attach/embed associated documents) security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status?)	Security & Complaince control status information is available to all clients upon request.

Facility Security					
Facility Security	Policy	FS-01	FS-01.1	Can you provide (describe/explain/attach/embed associated documents) evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Yes. Accela enforces policies and standards that comply with the NIST 800-53 family of controls.
Facility Security	User Access	FS-02	FS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes. Per Accela Background Check policy, background checks are conducted on all permanent employees and contractors.
Facility Security	Controlled Access Points	FS-03	FS-03.1	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Yes. All data centers and work areas have standard physical controls in place. Data centers comply with SSAE 16 compliance.
Facility Security	Secure Area Authorization	FS-04	FS-04.1	Do you allow (describe/explain/attach/embed associated documents) tenants to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	No. Accela carefully selects georgraphical locations for services and data based on numerous factors, including throughput associated with physical distance and client-load patterns.

Facility Security	Unauthorized Persons Entry	FS-05	FS-05.1	Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?	Yes. Accela enforces policies and standards that comply with the NIST 800-53 family of controls.
Facility Security	Offsite Authorization	FS-06	FS-06.1	Do you provide (describe/explain/attach/embed associated documents) tenants with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)	Yes. Accela enforces policies and standards that comply with NIST 800-53, Physical and Environmental Protection (PE) security controls.
Facility Security	Offsite equipment	FS-07	FS-07.1	Do you provide (describe/explain/attach/embed associated documents) tenants with documentation describing your policies and procedures governing asset management and repurposing of equipment?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Media Protection (MP) security controls.
Facility Security	Asset Management	FS-08	FS-08.1	Do you maintain a complete inventory of all of your critical assets, which includes ownership of the asset?	Yes All critical assets are maintained in the Configuration Management Database (CMDB) and updated throughthe use of Accela's Change Managemeent process.
Facility Security			FS-08.2	Do you maintain a complete inventory of all of your critical supplier relationships?	Yes. Our contract management function maintains this list.
Human Resources Security					
Human Resources Security	Background Screening	HR-01	HR-01.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification? What is checked during the background verification?	Yes. Per Accela Background Check policy, background checks are conducted on all permanent employees and contractors.
	Employment Agreements	HR-02	HR-02.1	Do you specifically train your employees regarding their role vs.	Yes. All Accela employees are required to participate in required, annual Security and Complaince awareness classes.

Human Resources Security				the tenant's role in providing information security controls?	
			HR-02.2	Do you document employee acknowledgment of training they have completed?	Yes. This is systematically captrured in our centralized training system.
Human Resources Security	Employment Termination	HR-03	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?	Yes.
Information Security					
Information Security	Management Program	IS-01	IS-01.1	Do you provide (describe/explain/attach/embed associated documents) tenants with documentation describing your Information Security Management Program (ISMP)?	Yes. Various security and compliance artifacts, including security control status, Plaon of Action and Milestones (POAM), and various types of complaince reports or attestation of compliance (AOC) are available upon request
Information Security	Management Support / Involvement	IS-02	IS-02.1	Are policies (describe/explain/attach/embed associated documents) in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?	Yes. Accela publishes and maintains and Information Technology and Security Standards documentation that is distributed to all applicable team members. Executive management reviews and approves security and complaince roadmaps and POAMS.
Information Security	Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular	Yes. Thety are aligned with NIST 800-53, PCI and SSAE 16 controls.

				industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	
			IS-03.2	Do you have (describe/explain/attach/embed associated documents) agreements, which ensure your providers adhere to your information security and privacy policies?	Yes. Accela has Interconnect Agreements in place.
			IS-03.3	Can you provide (describe/explain/attach/embed associated documents) evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	Yes. Detailed control status and POAM's are available upon request.
Information Security	Baseline Requirements	IS-04	IS-04.1	Do you have (describe/explain/attach/embed associated documents) documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	Yes. Baselines are documented for critical components. These baselines are reviewed and potentially adjusted annualy.
Information Security			IS-04.2	Do you have (describe/explain/attach/embed associated documents) a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes. Accela's internal audit function regularly audits security controls and reports results, which consequently transition into a Plan of Action and Milestone (POAM).
Information Security			IS-04.3	Do you allow (describe/explain/attach/embed associated documents) your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	No.
Information Security	Policy Reviews	IS-05	IS-05.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	No. However, Accela's security and complaince status are readiuly available for client review.

Information Security	Policy Enforcement	IS-06	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes. This is specifically managed Human Resources and the resource manager.
Information Security			IS-06.2	Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?	Yes.
Information Security	User Access Policy	IS-07	IS-07.1	Do you have (describe/explain/attach/embed associated documents) controls in place ensuring timely removal of systems access, which is no longer required for business purposes?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Access Control (AC) security controls.
Information Security			IS-07.2	Do you provide (describe/explain/attach/embed associated documents) metrics that track the speed with which you are able to remove systems access which is no longer required for business purposes?	Yes. Timely deactivation of accounts is governed by policy.

Information Security	User Access Restriction / Authorization	IS-08	IS-08.1	Do you document how you grant and approve access to tenant data?	Internal access requests from Accela team members is reviewed through the use of the change management process and explicit approval is required by the Change Management Review Board (CMRB). All change management activity is recorded using an enterprise change management tool.
Information Security			IS-08.2	Do you have (describe/explain/attach/embed associated documents) a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes. Accela adhered to a data classification methodology.
Information Security	User Access Revocation	IS-09	IS-09.1	Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	Yes. Timely deactivation of accounts is governed by policy.
Information Security			IS-09.2	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes. Status changes requiring access review include termination, role change or department transfer.
Information Security	User Access Reviews	IS-10	IS-10.1	Do you require at least annual certification of entitlements for all system users and administrators	Yes. Accela adhered to bi-annual and annual policy, procedure and standards review, which includes entitlements.

				(exclusive of users maintained by your tenants)?	Yes. The incident and change management processes are used.
Information Security			IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes.
Information Security			IS-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	
Information Security	Training / Awareness	IS-11	IS-11.1	Do you provide (describe/explain/attach/embed associated documents) or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	Yes. All Accela employees are required to participate in required, annual Security and Complaince awareness classes.
Information Security			IS-11.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Information Security	Industry Knowledge / Benchmarking	IS-12	IS-12.1	Do you participate in industry groups and professional associations related to information security?	Yes. Some of the groups Accela is associated with are ISACA, $(ISC)^2$, NIST, US-Cert.
			IS-12.2	Do you benchmark your security controls against industry standards?	Yes. NIST 800-53 and PCI are reviewed on a continuous basis by our internal audit team for compliance. External audits are conducted annualy.
Information Security	Roles / Responsibilities	IS-13	IS-13.1	Do you provide (describe/explain/attach/embed associated documents) tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant?	Yes.

Information Security	Management Oversight	IS-14	IS-14.1	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?	Yes. Security policies and procedures are reviewed annually with managers. Managers are expected to deessiminate relevant information to staff.
Information Security	Segregation of Duties	IS-15	IS-15.1	Do you provide (describe/explain/attach/embed associated documents) tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes. Information is available upon request.
Information Security	User Responsibility	IS-16	IS-16.1	How are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	Accela uses the Security and Compliance awareness program to achieve this goal. Additionally, meetings are help on as needed nasis to review policies with stakeholders, especially if material changes have been made to these documents.
Information Security			IS-16.2	How are users made aware of their responsibilities for maintaining a safe and secure working environment?	Accela uses the Security and Compliance awareness program to achieve this goal.
Information Security			IS-16.3	How are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	Accela communicates these requirements through the on-boarding process and is governed by security policies.
Information Security	Workspace	IS-17	IS-17.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	Although this is not explicitly addressed within our policies, however, Accela is committed to remediating any SLA/service conflicts with our clients. To date, this has not been an area of contention or conflict with our clients.
Information Security			IS-17.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Yes. Data integrity algorithms are enforce. Log activity is also monitored on a periodic basis.
Information Security			IS-17.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the	Yes. Baselines are defined and used to detect changes to the build/configuration of the VM's

				build/configuration of the virtual machine?	
Information Security	Encryption	IS-18	IS-18.1	Do you have (describe/explain/attach/embed associated documents) a capability to allow creation of unique encryption keys per tenant?	Encryption keys are not unique per tenant.
Information Security			IS-18.2	Do you support (describe/explain/attach/embed associated documents) tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (E.g. Identity based encryption)?	No. This is not practical in a multi-tenant environment with shared data stores.
Information Security	Encryption Key Management	IS-19	IS-19.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes. Data at rest and in transit are encypted.
Information Security			IS-19.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes.
Information Security			IS-19.3	Do you have (describe/explain/attach/embed associated documents) a capability to manage encryption keys on behalf of tenants?	Yes.
Information Security			IS-19.4	Do you maintain key management procedures?	Yes. This is integrated into Accela Information Technology and Security Standards.
Information Security	Vulnerability / Patch Management	IS-20	IS-21.1	Do you conduct (describe/explain/attach/embed associated documents) network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes. This is conducted on a monthly basis.
Information Security			IS-20.2	Do you conduct (describe/explain/attach/embed associated documents) application-layer vulnerability scans regularly as	Yes. This is conducted on an annual basis or as deemed necessary due to signifincat changes.

				prescribed by industry best practices?	
Information Security			IS-20.3	Do you conduct (describe/explain/attach/embed associated documents) local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes. This is conducted on a monthly basis.
Information Security			IS-20.4	Will you make the results of vulnerability scans available to tenants at their request?	High-level summary of findings, along with general remediation plans may be made available to tenants upon request. Detailed vulnerability scan and penetration test results are general not available due to the sensitive nature of this information.
Information Security			IS-20.5	Do you have (describe/explain/attach/embed associated documents) a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	Yes. This is systematically perfomed on a regular basis.
Information Security			IS-20.6	Will you provide your risk-based systems patching timeframes to your tenants upon request?	Yes.
Information Security	Antivirus / Malicious Software	IS-21	IS-21.1	Do you have (describe/explain/attach/embed associated documents) anti-malware programs installed on all systems that support your cloud service offerings?	Yes. These programs are updated on a regular basis.
Information Security			IS-21.2	Do you ensure that security threat detection systems that use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?	Accela has IDS capabilities deployed in a limited fashion. Accela's IDS capabilities is currently under review. The goal is to define an enterprise strategy across all data centers., m.
Information Security	Incident Management	IS-22	IS-22.1	Do you have (describe/explain/attach/embed associated documents) a documented security incident response plan?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Incident Response (IR) security controls.

Information Security			IS-22.2	Do you integrate customized tenant requirements into your security incident response plans?	Accela is committed to continuous improvement of the IR processes and welcomes client feedback that may be incorporated as enterprise standards.
Information Security			IS-22.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Tennant responsibilities are not included yet. This will be considered in the roles and responsibilities section of a futire version of the IR policy.
Information Security	Incident Reporting	IS-23	IS-23.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	Yes. BI tools are used against the merged results to conduct analysis and generate trending data.
Information Security			IS-23.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes.
Information Security	Incident Response Legal Preparation	IS-24	IS-24.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Incident Response (IR) security controls.
Information Security			IS-24.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes.
Information Security			IS-24.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	Yes. Point in time archives may be completed for this purpose.
Information Security			IS-24.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes. Tenant data separation is accomplished through the use of logical controls.
Information Security	Incident Response Metrics	IS-25	IS-25.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	Yes. The IR ifecycle includes, identification, validation, inpact anaylsis and after-incident debriefs.
Information Security			IS-25.2	Will you share statistical information security incident data with your tenants upon request?	Yes.

Information Security	Acceptable Use	IS-26	IS-26.1	Do you provide (describe/explain/attach/embed associated documents) documentation regarding how you may utilize or access tenant data and/or metadata?	Yes. Accela discloses how it uses tenant data. Tennat data is not sold or shared with external entities unles required by law.
Information Security			IS-26.2	Do you collect or create metadata about tenant data usage through the use of inspection technologies (search engines, etc.)?	Yes. This is mainly done to help with product and feature roadmaps.
Information Security			IS-26.3	Do you allow (describe/explain/attach/embed associated documents) tenants to opt-out of having their data/metadata accessed via inspection technologies?	No, since this is performed strictly for Accela-internal use and to help improve the product.
Information Security	Asset Returns	IS-27	IS-27.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have affected their data?	Yes.
Information Security			IS-27.2	Is your Privacy Policy aligned with industry standards? What standards are they aligned to?	Yes. Nist 800-53 security and privacy controls.
Information Security	e-commerce Transactions	IS-28	IS-28.1	Do you provide (describe/explain/attach/embed associated documents) open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)	Yes.

Information Security			IS-28.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?	Yes.
Information Security	Audit Tools Access	IS-29	IS-29.1	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Yes. Only select roles are granted access to these coponents.
Information Security	Diagnostic / Configuration Ports Access	IS-30	IS-30.1	Do you utilize dedicated secure networks to provide management access to your cloud service infrastructure?	Yes.
Information Security	Network / Infrastructure Services	IS-31	IS-31.1	Do you collect capacity and utilization data for all relevant components of your cloud service offering?	Yes.
Information Security			IS-31.2	Do you provide (describe/explain/attach/embed associated documents) tenants with capacity planning and utilization reports?	Capacity planning and utilization reports are internally monitored to provide clients with adequate support and resources. This information may be made available upon request.

Information Security	Portable / Mobile Devices	IS-32	IS-32.1	Are policies (describe/explain/attach/embed associated documents) and procedures established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Media Protection (MP) security controls.
Information Security	Source Code Access Restriction	IS-33	IS-33.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Yes. Access control is role based and carefully monitored. Access rights are audited on a periodic basis.
Information Security			IS-33.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Yes. Access control is role based and carefully monitored. Access rights are audited on a periodic basis.
Information Security	Utility Programs Access	IS-34	IS-34.1	Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	Yes. Access control is role based and carefully monitored. Access rights are audited on a periodic basis.
Information Security			IS-34.2	Do you have (describe/explain/attach/embed associated documents) a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?	The virtual infrastructure is not a component of the presentation layer. ESXi firewalls are in place with limited open ports. ESXi 6 hardening methods are generally used which serve as prenetative measures against threats such as "blue pill".

Information Security			IS-34.3	Are attacks that target the virtual infrastructure prevented with technical controls?	Yes.
Legal					
Legal	Nondisclosure Agreements	LG-01	LG-01.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Yes, these items are documented and reviewed on planned intervals.
Legal	Third Party Agreements	LG-02	LG-02.1	Do you select and monitor outsourced providers to verify that they comply with laws in the country where the data is processed and stored and transmitted?	Legal places requirements in contracts that are passed through for these types of data issues, and our provides comply.
Legal			LG-02.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Yes, we address for Canada and the United States. The Mideast and SOPAC are managed separately.
Legal			LG-02.3	Does legal counsel review all third party agreements?	Yes, legal reviews.
Operations Management					
Operations Management	Policy	OP-01	OP-01.1	Are policies (describe/explain/attach/embed associated documents) and procedures established and made available for all personnel to adequately support services operations roles?	Yes. Polcies and standards are periodically reviewed with personnel and are also made available post-review.

Operations Management	Documentation	OP-02	OP-02.1	Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuring, installing, and operating the information system is completed and performed correctly?	Yes. System documentation is periodically reviewed with personnel and are also made available post-review. Secuirty baselines have been established and incorporated into Information Technology and Security standards.
Operations Management	Capacity / Resource Planning	OP-03	OP-03.1	Do you provide (describe/explain/attach/embed associated documents) documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	No.
Operations Management			OP-03.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	Yes, however, these limits are usually not reached.
Operations Management	Equipment Maintenance	OP-04	OP-04.1	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities?	Yes.
Operations Management			OP-04.2	If using virtual infrastructure, Do you provide (describe/explain/attach/embed associated documents) tenants with a capability to restore a Virtual Machine to a previous state in time?	Tenant data may be restored to particular point in time.
Operations Management			OP-04.3	If using virtual infrastructure, Do you allow (describe/explain/attach/embed associated documents) virtual	No. This is shared environment with multiple tenants.

				machine images to be downloaded and ported to a new cloud provider?	
Operations Management			OP-04.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	No.
Operations Management			OP-04.5	Does your cloud solution include software / provider independent restore and recovery capabilities?	Yes.
Risk Management					
Risk Management	Program	RI-01	RI-01.1	Is your organization insured by a 3rd party for losses?	
Risk Management			RI-01.2	Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?	We do provide downtime credits for unplanned unavailability for Subscription/Hosting per those standard agreements.
Risk Management	Assessments	RI-02	RI-02.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes. Risk assesmenst are conducted in tandem with internal, external audits.
Risk Management			RI-02.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	Yes, but not using formal methods.

Risk Management	Mitigation / Acceptance	RI-03	RI-03.1	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?	Yes. In areas where company-wide criteria is not pre-defined, management reviews risks on an as-needed basis.
		RI-03	RI-03.2	Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?	Yes. In areas where company-wide criteria is not pre-defined, management reviews remediation plans and residual risk on an as-needed basis.
Risk Management	Business / Policy Change Impacts	RI-04	RI-04.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Risk assessments are evaluation and consequently, a remediation plan is developed and managed to completion. Annual reviews are conducted to maintain relevance with policies and standards.
Risk Management	Third Party Access	RI-05	RI-05.1	Do you provide (describe/explain/attach/embed associated documents) multi-failure disaster recovery capability?	Yes this is included in Accela's Business Continuity Plan (BCP).
			RI-05.2	Do you monitor service continuity with upstream providers in the event of provider failure?	Accela works closely with service providers during and post incident activity.
			RI-05.3	Do you have (describe/explain/attach/embed associated documents) more than one provider for each service you depend on?	Yes for infrastructure, critical components and services.
			RI-05.4	Do you provide (describe/explain/attach/embed associated documents) access to operational redundancy and continuity summaries that include the services on which you depend?	Yes, upon request.
			RI-05.5	Do you provide (describe/explain/attach/embed associated documents) the tenant the ability to declare a disaster?	No, however, the client may be a key stakeholder to validate a declaration of a disaster depending the extent, location and impact of such an event.

			RI-05.6	Do you provide (describe/explain/attach/embed associated documents) a tenant triggered failover option?	No. Failover options are managed by Accela personnel.
			RI-05.7	Do you share your business continuity and redundancy plans with your tenants?	Yes upon request.
Release Management					
Release Management	New Development / Acquisition	RM-01	RM-01.1	Are policies (describe/explain/attach/embed associated documents) and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	Yes. Accela enforces policies and standards that comply with NIST 800-53, Service Acquisition (SA) security controls.
Release Management	Production Changes	RM-02	RM-02.1	Do you provide (describe/explain/attach/embed associated documents) tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	Yes, upon request
Release Management	Quality Testing	RM-03	RM-03.1	Do you provide (describe/explain/attach/embed associated documents) your tenants with documentation which describes your quality assurance process?	Yes, upon request.
Release Management	Outsourced Development	RM-04	RM-04.1	Do you have (describe/explain/attach/embed associated documents) controls in place to ensure that standards of	Yes. They are available for review upon request.

				quality are being met for all software development?	
Release Management			RM-04.2	Do you have (describe/explain/attach/embed associated documents) controls in place to detect source code security defects for any outsourced software development activities?	Yes. Detailed code walk-throughs are part of our security review process.
Release Management	Unauthorized Software Installations	RM-05	RM-05.1	Do you have (describe/explain/attach/embed associated documents) controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes. This is governed by policy. Additionally, periodic review of software and system configurations (bi-annual and annual, depending on the subject area).
Resiliency					
Resiliency	Management Program	RS-01	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?	Yes. Accela has Business Continuity Process (BCP) and Disaster Recovery (DR) plans enforce.
Resiliency	Impact Analysis	RS-02	RS-02.1	Do you provide (describe/explain/attach/embed associated documents) tenants with ongoing visibility and reporting into your operational Service Level Agreement (SLA) performance?	Yes. This is available upon request.
Resiliency			RS-02.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	This capability is currently under development.

Resiliency			RS-02.3	Do you provide (describe/explain/attach/embed associated documents) customers with ongoing visibility and reporting into your SLA performance?	Yes. This is available upon request.
Resiliency	Business Continuity Planning	RS-03	RS-03.1	Do you provide (describe/explain/attach/embed associated documents) tenants with geographically resilient hosting options?	Yes. Accela has established a DR plan that includes a geographically, separate DR data center.
Resiliency			RS-03.2	Do you provide (describe/explain/attach/embed associated documents) tenants with infrastructure service failover capability to other providers?	Accela manages all infrastructure failover capabilities, including ones associated with services provided by other providers.
Resiliency	Business Continuity Testing	RS-04	RS-04.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes. Accela tests a variety of plans on an annual basis, incuding Incident Response and related plans such as BCP and DR.
Resiliency	Environmental Risks	RS-05	RS-05.1	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?	Yes. This is incorporated in Accela's Business Continuity Plan (BCP).
Resiliency	Equipment Location	RS-06	RS-06.1	Are any of your datacenters located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	No. Accela has taken great care in selecting production and disaster recovery data centers.

Resiliency	Equipment Power Failures	RS-07	RS-07.1	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes. Comprehensive power redundancy is in place.
Resiliency	Power / Telecommunications	RS-08	RS-08.1	Do you provide (describe/explain/attach/embed associated documents) tenants with documentation showing the transport route of their data between your systems?	Not usually, however, this is an area that may be revisited especially I the context of a related incident. All network traffic is constrained to continental United States.
Resiliency			RS-08.2	Can Tenants define how their data is transported and through which legal jurisdiction?	No. All network traffic is constrained to continental United States.
Security Architecture					
Security Architecture	Customer Access Requirements	SA-01	SA-01.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	Yes.
Security Architecture	User ID Credentials	SA-02	SA-02.1	Do you support (describe/explain/attach/embed associated documents) use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Not at the moment, however, this is actively being pursued and it is on the product roadmap.
Security Architecture			SA-02.2	Do you use open standards to delegate authentication capabilities to your tenants?	Yes.
Security Architecture			SA-02.3	Do you support (describe/explain/attach/embed associated documents) identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Not at the moment, however, this is actively being pursued and it is on the product roadmap.
Security Architecture			SA-02.4	Do you have (describe/explain/attach/embed associated documents) a Policy Enforcement Point capability (ex.	Accela uses Active Directory (AD).

				XACML) to enforce regional legal and policy constraints on user access?	Although role-based identity management is in place, it is not done systematically, yet. Not at the moment, however, this is actively being pursued and it is on the product roadmap.
Security Architecture			SA-02.5	Do you have (describe/explain/attach/embed associated documents) an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?	Agency administrators can restrict users in the system to groups which have different levels of functionality and access.
Security Architecture			SA-02.6	Do you provide (describe/explain/attach/embed associated documents) tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc.) for user access?	Not in the hosted environment.
Security Architecture			SA-02.7	Do you allow (describe/explain/attach/embed associated documents) tenants to use third party identity assurance services?	We don't have any in the hosted environment using this. SSO adapters in an on-premise setting may provide that depending on the use case.
Security Architecture	Data Security / Integrity	SA-03	SA-03.1	Is your Data Security Architecture designed using an industry standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)	We are working towards a FISMA (NIST 800-53) compliancy audit date 10/16.

Security Architecture	Application Security	SA-04	SA-04.1	Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)?	We are working towards a FISMA (NIST800-53) compliancy audit date 10/16.
Security Architecture			SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?	HP WebInspect is used during the development process to detect issues.
Security Architecture			SA-04.3	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	
Security Architecture	Data Integrity	SA-05	SA-05.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	There is basic data input validation. Additionally, administrators can create custom expressions for other types of extended validaation.
Security Architecture	Production / Nonproduction Environments	SA-06	SA-06.1	For your SaaS or PaaS offering, Do you provide (describe/explain/attach/embed associated documents) tenants with separate environments for production and test processes?	Yes, each tenant gets two other environments (support, test) along with production.
Security Architecture			SA-06.2	For your IaaS offering, Do you provide (describe/explain/attach/embed associated documents) tenants with guidance on how to create suitable production and test environments?	Yes, our Customer Support and Services teams can help with these.

Security Architecture	Remote User Multifactor Authentication	SA-07	SA-07.1	Is multi-factor authentication required for all remote user access?	Yes
Security Architecture	Network Security	SA-08	SA-08.1	For your IaaS offering, Do you provide (describe/explain/attach/embed associated documents) customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	We can provide information on network communication for all endpoints such that the architecture can be built.
Security Architecture	Segmentation	SA-09	SA-09.1	Are system and network environments logically separated to ensure Business and customer security requirements?	Yes
Security Architecture			SA-09.2	Are system and network environments logically separated to ensure compliance with legislative, regulatory, and contractual requirements?	Yes
Security Architecture			SA-09.3	Are system and network environments logically separated to ensure separation of production and non-production environments?	Yes, production and non-production environments use their own independent resources.

Security Architecture			SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?	Yes
Security Architecture	Wireless Security	SA-10	SA-10.1	Are policies (describe/explain/attach/embed associated documents), procedures established, and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?	Yes
Security Architecture			SA-10.2	Are policies (describe/explain/attach/embed associated documents) and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)	Yes
Security Architecture			SA-10.3	Are policies (describe/explain/attach/embed associated documents) and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue)	Yes

				network devices for a timely disconnect from the network?	
Security Architecture	Shared Networks	SA-11	SA-11.1	Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards? Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations. Provide information about your plan.	Yes
Security Architecture	Clock Synchronization	SA-12	SA-12.1	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	Yes
Security Architecture	Equipment Identification	SA-13	SA-13.1	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?	No, equipment is not identified in an automated fashion.
Security Architecture	Audit Logging / Intrusion Detection	SA-14	SA-14.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Yes
Security Architecture			SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?	Yes
Security Architecture			SA-14.3	Can you provide (describe/explain/attach/embed associated documents) evidence that due diligence mapping of regulations and standards to your	Yes, our System Security Plan, which is used within our NIST 800-53 controls for FISMA, is evidenice of our due dillegence in regards to security controls.

				controls/architecture/processes has been done?	
Security Architecture	Mobile Code	SA-15	SA-15.1	Is mobile code authorized before its installation and use? Is the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes
Security Architecture			SA-15.2	Is all unauthorized mobile code prevented from executing?	Yes

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT H

ACCELA SUBSCRIPTION TERMS AND CONDITIONS

Version 52615a

1. As used herein, "Accela" refers to Accela, Inc. and "Customer" refers to the subscribing customer designated on the attached Order. Accela and Customer are collectively designated as the "Parties".

2. These Subscription Terms and Conditions ("Terms") are effective upon execution of the Order by Customer and are for the exclusive benefit of the Parties. Nothing herein will be construed to create any benefits, rights, or responsibilities in any other parties.

3. Customer's subscription term commences on the date set forth in the body of the Agreement.

4. Subscription terms are twelve (12) calendar months in duration. At the end of Customer's subscription term or, if a multi-term subscription is indicated on the Order, the last of Customer's subscription terms, Customer's may renew subscription as set forth in the Agreement. The per-unit pricing during said additional term will be the same as the prior term's annual fees unless Accela notifies Customer otherwise not less than sixty (60) calendar days prior to the end of said prior term and Customer agrees to the change in pricing in writing. Any price increase will be effective at the start of the renewal term, subject to Customer's budget appropriations and approvals. No such price increase will exceed three percent (3%) of the prior term's annual pricing.

5. In exchange for its use of the Subscribed Services, Customer will pay to Accela the amounts indicated in the Order. Said amounts are based on services purchased and not actual usage; payment obligations are non-cancelable and fees paid are non-refundable, except as otherwise specifically-provided herein. Unless otherwise stated, such fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including but not limited to value-added, sales, use or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction ("Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If Accela has the legal obligation to pay or collect Taxes for which Customer is responsible, the appropriate amount will be invoiced to and paid by Customer, unless Accela is provided with a valid tax exemption certificate authorized by the appropriate taxing authority. Accela is solely responsible for taxes assessable against it based on its income, property, employees, and as set forth in Section 8 of this Agreement.

6. The Subscribed Services are protected under the laws of the United States and the individual states and by international treaty provisions. Accela retains full ownership in the Subscribed Services and grants to Customer a limited, nonexclusive, nontransferable right to use the Subscribed Services, subject to the following terms and conditions: a) The Subscribed Services are provided for use only by Customer employees and to the extent of their duties for Customer, Customer's agents, contractors and officials; b) Customer may not make any form of derivative work from the Subscribed Services, although Customer is permitted to develop additional or alternative functionality for the Software using tools and/or techniques provided to Customer by Accela; c) Customer may not obscure, alter, or remove any confidentiality or proprietary rights notices; d) Customer may use the Subscribed Services only to process transactions relating to properties within both its own geographical and political boundaries and may not sell, rent, assign, lend, or

share any of its rights hereunder; e) Customer is responsible for all activities conducted using its user credentials and for its users' compliance with the provisions of these Terms; and f) All rights not expressly granted to Customer are retained by Accela. Accela will make the Subscribed Services available to Customer pursuant to these Terms during a subscription term. Customer agrees that its purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by Accela regarding future functionality or features.

7. Accela warrants that it has full power and authority to agree to these Terms and that, as of the effective date hereof, the Subscribed Services do not infringe on any existing intellectual property rights of any third party. If a third party claims that the Subscribed Services do infringe, Accela may, at its sole option, secure for Customer the right to continue using the Subscribed Services or modify the Subscribed Services so that these do not infringe. Accela will have the sole right to conduct the defense and will defend any legal action and conduct all negotiations for its settlement or compromise.

8. **WARRANTIES AND DISCLAIMERS**

8.1 Specifications. Accela shall be responsible for the acquisition and operation of all network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of Accela. The system shall be available 24/7/365 (with agreed-upon maintenance downtime) and provide service to customer as defined in the SLC set forth in section 8.2 of this Exhibit. Subject to the limitations set forth below, Accela warrants that the Service will operate in all material respects in accordance with the Specifications. As Customer's sole and exclusive remedy and Accela's entire liability for any breach of the foregoing warranty, Accela will use commercially reasonable efforts to modify the Service so that it conforms to foregoing warranty.

8.2 Service Level Commitment. During the Subscription Period, Accela further warrants that the Service will meet the performance level specified in the Service Level Commitment, as made available by Accela in the Attachment A to Exhibit I. The Service Level Commitment sets forth Customer's sole and exclusive remedy for Accela's failure to achieve the stated Service performance level.

8.3 Disclaimers. EXCEPT AS EXPRESSLY PROVIDED HEREIN, ACCELA DOES NOT MAKE ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND ACCELA SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES ARISING OUT OF THE COURSE OF DEALING OR USAGE OF TRADE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. Accela will not be responsible to the extent failure of the Service to operate as warranted is caused by or results from: (i) any modification to the Service other than a Supported Modification; (ii) combination, operation or use of the Service with Customer's or a third party's applications, software or systems; (iii) abuse, willful misconduct or negligence by anyone other than Accela or Accela's designee; (iv) use of

the Service other than in accordance with the terms of this Agreement and/or the applicable Specifications and Accela documentation or (v) any of the SLC Exclusions (as defined in the Service Level Commitment).

8.4 **MUTUAL INDEMNIFICATION**

8.5 Indemnification by Customer. Customer will defend (or settle), indemnify and hold harmless Accela, its officers, directors, employees and subcontractors, from and against any liabilities, losses, damages and expenses, including court costs and reasonable attorneys' fees, arising out of or in connection with any third-party claim that: (i) a third party has suffered injury, damage or loss resulting from Customer's or any End User's use of the Service (other than any claim for which Accela is responsible under Section 7.2); or (ii) Customer or any End User has used the Service in a manner that violates these Terms or applicable law. Customer's obligations under this Section 7.1 are contingent upon: (a) Accela providing Customer with prompt written notice of such claim; (b) Accela providing reasonable cooperation to Customer, at Customer's expense, in defense and settlement of such claim; and (c) Customer having sole authority to defend or settle such claim.

8.6 Indemnification by Accela. Accela will defend (or settle) any suit or action brought against Customer to the extent that it is based upon a claim that the Service, as furnished by Accela hereunder, infringes or misappropriates the Intellectual Property Rights of any third party, and will pay any costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against Customer. Accela's obligations under this Section 7.2 are contingent upon: (a) Customer providing Accela with prompt written notice of such claim; (b) Customer providing reasonable cooperation to Accela, at Accela's expense, in the defense and settlement of such claim; and (c) Accela having sole authority to defend or settle such claim. THIS SECTION 9.2 STATES THE ENTIRE OBLIGATION OF ACCELA AND ITS LICENSORS WITH RESPECT TO ANY ALLEGED OR ACTUAL INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS BY THE SERVICE. Accela will have no liability under this Section 9.2 to the extent that any third-party claims described herein are based on any combination of the Service with products, services, methods, or other elements not furnished by Accela, or any use of the Service in a manner that violates this Agreement or the instructions given to Customer by Accela.

8.7 Mitigation Measures. In the event that (i) any claim or potential claim covered by Section 9.2 arises or (ii) Accela's right to provide the Service is enjoined or in Accela's reasonable opinion is likely to be enjoined, Accela may, in its discretion, seek to mitigate the impact of such claim or injunction by obtaining the right to continue providing the Service, by replacing or modifying the Service to make it non-infringing, and/or by suspending or terminating Customer's use of the Service with reasonable notice to Customer. In the case of a suspension or termination pursuant to this Section 7.3, Accela will refund to Customer a portion of fees prepaid by Customer for the then-current Subscription period, prorated to the portion of that Subscription period that is affected by the suspension or termination).

9 **LIMITATIONS OF LIABILITY.** IN NO EVENT WILL ACCELA'S AGGREGATE LIABILITY TO CUSTOMER OR ANY THIRD PARTY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR FROM THE USE OF OR INABILITY TO USE THE SERVICE, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER HEREUNDER OR, WITH RESPECT TO ANY SINGLE INCIDENT, THE AMOUNT PAID BY CUSTOMER DURING THE SUBSCRIPTION PERIOD UNDER WHICH INCIDENT OCCURS.

9.1 Exclusion of Damages. NEITHER ACCELA NOR ANY OTHER PERSON OR ENTITY INVOLVED IN CREATING, PRODUCING, OR DELIVERING THE SERVICE WILL BE LIABLE FOR ANY INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, LOSS OF DATA OR LOSS OF GOODWILL, SERVICE INTERRUPTION, COMPUTER DAMAGE OR SYSTEM FAILURE OR THE COST OF SUBSTITUTE PRODUCTS OR SERVICES, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR FROM THE USE OF OR INABILITY TO USE THE SERVICE, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR ANY OTHER LEGAL THEORY. THE FOREGOING EXCLUSIONS APPLY WHETHER OR NOT ACCELA HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE, AND EVEN IF A LIMITED REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE. NOTHING IN THESE TERMS EXCLUDES OR RESTRICTS THE LIABILITY OF EITHER PARTY FOR DEATH OR PERSONAL INJURY RESULTING FROM ITS NEGLIGENCE.

9.2 Security and Other Risks. Customer acknowledges that, notwithstanding security features of the Service, no product, hardware, software or service can provide a completely secure mechanism of electronic transmission or communication and that there are persons and entities, including enterprises, governments and quasi-governmental actors, as well as technologies, that may attempt to breach any electronic security measure. Subject only to its limited warranty obligations set forth in Section 6, Accela will have no liability for any security breach caused by any such persons, entities, or technologies.

9.3 Any Accela security patches for "Very High" and "High" severity level security risks will be available to customer and patched within thirty (30) days of patch availability. Accela defines a Very High severity level where the offending line or lines of code is a very serious weakness and is an easy target for an attacker. Accela defines High severity level where the offending line or lines of code have significant weakness.

9.4 Customer further acknowledges that the Service is not guaranteed to operate without interruptions, failures, or errors. If Customer or End Users use the Service in any application or environment where failure could cause personal injury, loss of life, or other substantial harm, Customer assumes any associated risks and will indemnify Accela and hold it harmless against those risks.

9.5 Data Breach Notification:
The service provider shall inform the Customer of any unauthorized and unlawful acquisition of unencrypted personal data ("Data Breach").

a. Data Breach Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Data Breach with the Customer should be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

b. Data Breach Reporting Requirements: If the service provider has actual knowledge of a confirmed Data Breach that affects the security of any Customer content that is subject to applicable Data Breach notification law, the service provider shall (1) promptly notify the appropriate Customer identified contact within 48 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach.

9.6 Basis of Bargain. THE LIMITATIONS OF LIABLITY AND EXCLUSIONS OF DAMAGES SET FORTH IN THIS SECTION 10 ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN ACCELA AND CUSTOMER AND WILL APPLY TO THE MAXIMUM EXTENT ALLOWED UNDER APPLICABLE LAW.

11. The following are not covered by these Terms, but may be separately available at rates and on terms which may vary from those described herein: a) Services required due to misuse of the Subscribed Services; b) Services required due to external factors including, but not necessarily limited to, Customer's use of software or hardware not authorized by Accela; or c) Services required to resolve or work-around conditions which cannot be reproduced in Accela's support environment.

12. Customer warrants that it owns or has been authorized to provide the data to Accela. Customer retains full ownership of said data and grants to Accela a limited, nonexclusive, nontransferable license to use said data only to perform Accela's obligations in accordance with these Terms.

13. Subject to the limitations of Section 6, Customer may authorize access to the Subscribed Services by creating unique user names and passwords ("Logins") up to the number of users indicated in the Order.

14. Each Login must be assigned to a single individual and may not be shared or used by more than one such user. Customer may reassign any Login to another individual, provided that such reassignments do not circumvent the "single individual" requirement described in this Section.

15. Customer acknowledges that transmissions and processing of Customer's electronic communications are fundamental to Customer's use of the Subscribed Services. Customer further acknowledges that portions of such transmissions and processing may occur within various computer networks not owned or operated by Accela. Customer agrees that Accela is not responsible for any delays, losses, alterations, interceptions, or storage of its electronic communications which occur in computer networks not owned or operated by Accela.

16. "Disclosing Party" and "Recipient" refer respectively to the party which discloses information and the party to which information is disclosed in a given exchange. Either Accela or Customer may be deemed Disclosing Party or Recipient depending on the circumstances of a particular communication or transfer of information. "Confidential Information" means all disclosed information relating in whole or in part to non-public data, proprietary data compilations, computer source codes, compiled or object codes, scripted programming statements, byte codes, or data codes, entity-relation or workflow diagrams, financial records or information, client records or information, organizational or personnel information, business plans, or works-in-progress, even where such works, when completed, would not necessarily comprise Confidential Information. The foregoing listing is not intended by the Parties to be comprehensive, and any information which Disclosing Party marks or otherwise designates as "Confidential" or "Proprietary" will be deemed and treated as Confidential Information. Information which qualifies as "Confidential Information" may be presented to Recipient in oral, written, graphic, and/or machine-readable formats. Regardless of presentation format, such information will be deemed and treated as Confidential Information. Notwithstanding, the following specific classes of information are not "Confidential Information" within the meaning of this Section: a) information which is in Recipient's possession prior to disclosure by Disclosing Party; b) information which is available to Recipient from a third party without violation of this Section or Disclosing Party's intellectual property rights; c) information which is in the public domain at the time of disclosure by Disclosing Party, or which enters the public domain from a source other than Recipient after disclosure by Disclosing Party; d) information which is subpoenaed by governmental or judicial authority; and e) information subject to disclosure pursuant to a state's public records laws. Recipient will protect the confidentiality of Confidential Information using the same degree of care that it uses to protect its own information of similar importance, but will in any case use no less than a reasonable degree of care to protect Confidential Information. Recipient will not directly or indirectly disclose Confidential Information or any part thereof to any third party without Disclosing Party's advance express written authorization to do so. Recipient may disclose Confidential Information only to its employees or agents under its control and direction in the normal course of its business and only on a need-to-know basis. In responding to a request for Confidential Information, Recipient will cooperate with Disclosing Party, in a timely fashion and in a manner not inconsistent with applicable laws, to protect the Confidential Information to the fullest extent possible.

Accela acknowledges that Customer is a public agency subject to the requirements of the California Public Records Act Cal. Gov. Code section 6250 et seq. Customer acknowledges that Accela may submit information to Customer that Accela considers

confidential, proprietary, or trade secret information pursuant the Uniform Trade Secrets Act (Cal. Civ. Code section 3426 et seq.), or otherwise protected from disclosure pursuant to an exemption to the California Public Records Act (Government Code sections 6254 and 6255). Accela acknowledges that Customer may submit to Accela information that Customer considers confidential or proprietary or protected from disclosure pursuant to exemptions to the California Public Records Act (Government Code sections 6254 and 6255). Upon request or demand of any third person or entity not a party to this Agreement ("Requestor") for production, inspection and/or copying of information designated by a Disclosing Party as Confidential Information, the Recipient as soon practical but within three (3) days of receipt of the request, shall notify the Disclosing Party that such request has been made, by telephone call, letter sent via facsimile and/or by US Mail to the address and facsimile number listed at the end of the Agreement. The Disclosing Party shall be solely responsible for taking whatever legal steps are necessary to protect information deemed by it to be Confidential Information and to prevent release of information to the Requestor by the Recipient. If the Disclosing Party takes no such action, after receiving the foregoing notice from the Recipient, the Recipient shall be permitted to comply with the Requestor's demand and is not required to defend against it.

17. **ACCELA WILL, AT ALL TIMES DURING THE AGREEMENT, MAINTAIN INSURANCE COVERAGE AS SET FORTH IN EXHIBIT C. TO THE EXTENT NOT OFFSET BY ITS INSURANCE COVERAGE AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS, IN NO EVENT WILL ACCELA'S CUMULATIVE LIABILITY FOR ANY GENERAL, INCIDENTAL, SPECIAL, COMPENSATORY, OR PUNITIVE DAMAGES WHATSOEVER SUFFERED BY CUSTOMER OR ANY OTHER PERSON OR ENTITY EXCEED THE FEES PAID TO ACCELA BY CUSTOMER DURING THE TWELVE (12) CALENDAR MONTHS IMMEDIATELY PRECEDING THE CIRCUMSTANCES WHICH GIVE RISE TO SUCH CLAIM(S) OF LIABILITY.**

18. If Accela is delayed in its performance of any obligation hereunder due to causes or effects beyond its control, Accela will give timely notice to Customer of such circumstances and will act in good faith to resume performance as soon as practicable.

19. Accela may not assign its rights and obligations hereunder for purposes of financing or pursuant to corporate transactions involving the sale of all or substantially all of its stock or assets without Customer's written consent.

20. Section 5 will survive the End of Term for so long as is required to complete collection of unpaid amounts. The limitations and waivers described in Sections 8, 19, and 21 will survive the End of Term. Section 12 will survive the End of Term for a period of thirty (30) calendar days. Section 16 will survive the End of Term for a period of thirty (30) calendar days or for so long as is required for Accela to complete its response to a Customer request made during said thirty-day period. Section 20 will survive the End of Term for a period of two (2) years. With the exceptions of the foregoing surviving sections, the remainder of these Terms will terminate at the End of Term.

AGREEMENT FOR THE PERFORMANCE OF SUBSCRIBED SERVICES
BY AND BETWEEN THE
CITY OF SANTA CLARA, CALIFORNIA,
AND
ACCELA, INC.

EXHIBIT I

ACCELA SECURITY EXHIBIT

Accela will provide hosting at a SSAE-16 Tier III or higher facility as defined by the Uptime Institute, Inc. Per the hosting datacenter's disclosure policies, Accela will provide, where allowable, a copy of the datacenter's annual SSAE-16 Type 2 audit report. Accela will provide a backup hosting site with equivalent status for disaster recovery should a major catastrophic outage occur.

The hosting facility will be constructed and configured to ensure reasonable and adequate protection of the equipment in the event of a natural event considered possible for the physical location, including but not limited to earthquake, flood, hurricane, tornado, etc.

Data Location:

> The service provider shall provide its services to the Customer and its end users solely from data centers in the U.S. Storage of Customer data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store Customer data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The service provider shall permit its personnel and contractors to access Customer data remotely only as required to provide technical support. The service provider may provide technical user support on a 24/7 basis using a Follow-the-Sun model, unless otherwise prohibited in the SLC listed in this Exhibit H.

The hosting facility must have power sufficient to support the equipment platform as configured; this includes provisions for back-up power supplies. The facility will include:

- Dual power availability to each rack unit from independent Power Distribution Units (PDUs) removes PDU loss as a single point of failure
- N+1 redundancy of uninterruptible power supplies
- Redundant fuel-based generator power supplies, in the event of a power failure from commercial power.

The hosting facility will have reasonable and adequate heating and cooling to insure continuous operation of equipment within acceptable operational limits. The hosting facility shall include but not be limited to the following features:

- N+1 redundancy of cooling towers, water pumps and chillers
- Multiple air handling units providing an additional level of redundancy

- Cooling units maintain consistent environment temperature and relative humidity levels
- Rack cabinet fans to circulate warm air generated by the servers

The hosting facility will have physical security to control unauthorized access to the equipment, including but not limited to:

- 24/7 on-site security guard
- Indoor and outdoor security monitoring
- Badge/picture ID access screening
- Biometric access screening
- Escort requirements for access to raised floor areas
- Logged entries for all users entering or leaving the premises

The hosting facility will have data line capacity to ensure responsive access to the proposed data system by Accela employees, jurisdictions and customers.

Accela shall provide the equipment, hardware and network infrastructure necessary to operate and sustain all contracted software on behalf of customer and to provide the necessary development, test, production, and training environments.

The hosting facility will provide secure encrypted transmission of personal data to include, but not limited to, personal name and address, SSN, credit card, banking, and payment data, passwords, and any other data subject to Federal or California State data privacy protection laws, and provide protection that meets or exceeds any such statutory requirements. Secure Socket Layer (SSL) encryption will be utilized to meet this requirement.

Accela will be responsible for the data communication infrastructure that connects the data servers to the communication network (switches, etc.)

Accela will maintain any service agreements for the equipment and operating systems, and maintain the equipment in optimal working order.

Accela shall provide a PCI compliant infrastructure for deployment within the data center. Accela's applications have been developed to comply with all 12 requirements of PCI Data Security Standard, including:

- The use of a firewall within the proposed infrastructure to protect cardholder data provided via both Accela Automation and Accela Citizen Access (public portal)
- The use of strong passwords and password policies to ensure password protection and delineates and enforces role-based security to ensure that only authorized users and administrators can access sensitive data
- The use of secured sessions to prevent any unauthorized access to sensitive cardholder data
- The use of encryption per PCI and PABP standards whenever cardholder data is transmitted across open, public networks
- Adherence to all applicable industry standards for the development of secure systems

and the Accela applications that operate within these systems

- The assignment of unique User IDs and Passwords for each user granted access to the system
- The provision of full audit trail tracking to track and monitor all access to network resources and cardholder data

Accela will provide operational services to support the infrastructure and operating environment.

Accela shall provide the equipment, hardware and network infrastructure necessary to operate and sustain all contracted software and to provide the necessary, production, support and staging environments.

Accela shall ensure there are no covert channels to access the system and must take precautions to protect the system and data from Trojan invasion.

Accela contracts for warranty services. In the event that warranty services are required, Accela shall provide staff support sufficient to complete all necessary service and maintenance to the hardware and software platform for the duration of a Vendor-site support agreement.

Accela shall perform daily backups of the data. The images that constitute the functional system will have snapshots taken weekly and stored to the fully redundant storage system. Accela's backup strategies and fully redundant Data Recovery (DR) site ensure that a complete system rebuild of data will not be necessary. Accela will use commercially reasonable efforts to replicate all relevant agency data "in near real-time" to a geographically separate location where we have the ability to stand up the Accela application stack and restore service.

Throughout the term of the agreement, upon the request of Customer, Accela will provide Customer with:

(i) a copy of its data in a database dump file
(ii) an APO property conversion upload
(iii) a Crystal Report placement

Within thirty (30) calendar days following the end of its final Subscribed Services term ("End of Term"), Accela shall provide a complete copy of Customer's data and associated documents, as updated or modified by Customer's use of the Subscribed Services, in a database dump file format. Accela will comply in a timely manner with such request, provided that Customer pays any and all unpaid amounts due to Accela.

Accela will meet measurable standards for expected and reasonable system availability (up-time) as established elsewhere in this Hosting Attachment. The system must generally be available seven days a week, twenty-four hours per day. Scheduled down time is acceptable. Unplanned down time between 6:00 am and 8:00 pm Pacific time must be to resolve production emergencies only, limited to no more than One Hundred and Twenty (120) minutes and occur no more than one time per month. In no event will any proposed standard be less than a commercially reasonable standard.

The Accela system implementation shall provide functional equivalents of the following environments; hardware and software requirements must include provisions to support these environments:

- Support – An environment available to customers to develop and test new configurations or changes to existing configurations prior to implementation in production.
- Staging – An environment available to customers to test new Accela Automation application releases against their production configuration. New application code will be deployed to the Staging environment within one week of becoming Generally Available (GA) from Engineering. New application code will be deployed to the Support and Production environments one month after being deployed to Staging for Major releases and two weeks for Minor releases (Service Packs).
- Production – The environment used by customers, jurisdiction staff, central administrative staff, and analysts/programmers to submit, track and manage live transactions and associated data.

The Customer shall have the ability to import or export data in piecemeal at its discretion without interference from the service provider. Accela will provide the customer with a full database export on a quarterly basis at the request of Customer. The customer has the option to request a more frequent export if desired, but will not exceed one per calendar week.

Accela will respond to requests for production or support/staging environment report posting within 72 hours of the request. Reports will be reviewed for system performance and data integrity before posting. If issues are found they will be documented and communicated back to the customer for correction. In the event that a report request is urgent, Accela will expedite this process to an extent that is reasonable for the request.

To provide the Hosting Services, Accela shall provide, host, manage and maintain the System as follows:

A. Management, Support and Maintenance of Hardware

1. Accela will provide, manage and maintain operating systems on all System environment hardware. This will involve application of any necessary patches or updates and upgrades as necessary. Accela will provide system redundancy.

2. Accela will provide, manage and maintain, for the System, the physical or virtual resources. This will involve any physical fix as needed, updates or refreshes as necessary.

B. Capacity Planning and Monitoring

Accela will be responsible for monitoring capacity and performing capacity planning to ensure the System environment has sufficient capacity to meet the service level agreements agreed upon in this Agreement.

C. Asset Management

Asset Management services provide inventory and tracking of equipment and the management of vendor-provided maintenance agreements.

Accela will perform the following tasks:

1. Manage third party vendor contracts for equipment used in support of this Agreement (rental agreements, leases, service agreements, warranties, amendments, maintenance contracts, and insurance policies)

2. Provide hardware and software at the appropriate hardware and software levels to comply with vendor maintenance contracts.

3. Provide an asset tracking tool to maintain a database of asset information such as make, model, operating system, number of CPUs, amount of memory, and amount of storage.

D. Facilities Services

Accela will provide a PCI-DSS compliant facility.

E. Monitoring Server and OS

1. Monitoring Server and OS service detects and responds to up/down availability faults generated by monitored servers.

2. Accela will perform the following:

- Provide the operational support processes required for up/down monitoring
- Document and track all detected problems using the site problem management process
- Escalate all detected problems to the appropriate support personnel

F. Operations Management

1. Operations Management are those activities requiring physical hands-on support. Accela shall provide skilled staff to support all operational support services at an Accela data center facility.

2. Accela will perform the following:
   - Perform systems operation functions such as power on/off and start/stop/reset device intervention
   - Monitor vendors on the Accela premise performing work maintenance or problem resolution work
   - Maintain responsibility for procuring any expendable supplies (CDs,

tapes, cleaning supplies, and so forth)

G. Operating System Management

1. Accela shall provide proper functionality of hosting software on servers. Support is provided for operating systems and related software products. Included are all ongoing processes to maintain supplier-supported operating platforms including preventive software maintenance services.

2. Accela will perform the following:

- Install and maintain system-level software, such as operating system and other system-level products software requiring user access
- Monitor system software status and take necessary action to resolve any issues
- Perform operation system software tuning as required to maintain daily operations for Accela-provided services
- Install preventive maintenance patches deemed critical by the vendor to support system software products to prevent known problems from impacting the operating environment
- Install patches per vendor instructions for security exposures deemed critical by the vendor
- Participate in the identification of connectivity and associated network problems
- Plan and implement necessary changes for the System
- Document and track all configuration management changes using the site change management process
- Provide problem escalation and interact as necessary with third-party suppliers

H. System/File Backup and Restore

1. System/File Backup and Restore Services provide the operational and management processes to backup and restore operating system.

2. Accela will perform the following:

- Design and implement the backup Plan
- Perform backups
- Provide for data restores as needed if Agency causes the need for a data restoration, Agency will be responsible for the cost of the data restore at the hourly service rate in the Contract.
- Monitor backup processes and verification of successful completion
- Adjust backup and restore plans as new components are added to the System

I. Server Storage Management

1. Server Storage Management provides for the support of server direct-attached storage environment.

2. Accela will perform to following:
   - Integrate the storage hardware and software to provide the appropriate level of capacity, scalability, and performance of the server storage hardware and software
   - Manage hardware and software maintenance requirements based on the manufacturer's recommended schedule
   - Implement security practices, such as logical unit masking, preventing unauthorized storage access from an unauthorized server
   - Maintain proper storage configuration(s) (mapping logical volumes, creating file systems, balancing I/O capacity)

J. Server Management Services

Accela will provide server management services.

K. Hardware Management

Accela will provide Hardware Management. Hardware management provides the services necessary to enable compute equipment to be physically installed, maintained, and kept operational.

L. Controlled Server Access

Accela will provide Controlled Server Access. Controlled server access provides the tools and processes to manage access to assets. This includes the management of user logon IDs and their access rights to system-level resources, as well as maintaining server-level security parameters and security product options.

M. Virus Protection

Accela will provide Virus Protection services. Server level anti-virus service provides anti- virus software on each server to provide protection and detection of viruses, worms, and other malicious code. The anti-virus software can be updated with current virus signatures and detection engines automatically or by file distribution software. This service also provides the means to scan the server at the system level to detect malicious code.

N. Security Event Logging

Accela will provide Security Event Logging. Security Event Logging is a detective control that enables the recording of security events on system hosts based on preset

parameters. The administrative tool's logging function is enabled and the security events are retained in a record for future review.

O. Vulnerability Scan and Report

Accela will provide Vulnerability management. Vulnerability management includes preventive and detective services to identify vulnerabilities as they emerge; to prevent those vulnerabilities from affecting the in-scope systems; to detect when an in-scope system has been affected; and to cure those affected systems. Vulnerability management includes both Vulnerability Alert management and Vulnerability Scanning processes. Vulnerability Alert management is the preventive process that collects known vulnerabilities and prioritizes vulnerabilities based on associated risk. Vulnerability Scanning is the detective process of identifying potential vulnerabilities on servers for exposures to such vulnerabilities.

P. Managed Cluster

Accela will provide Managed Cluster Management. Managed Cluster Management provides processes to deliver server/storage configurations clustered together in the same physical site. This is delivered through the use of hardware configuration and software to meet availability requirements.

Q. Host Based Intrusion Detection

Accela will provide Host Based Intrusion Detection. Host Based Intrusion Detection is the real-time identification, detection, and notification of suspected unauthorized intrusions on individual servers.

R. Secondary Mirrored Site Management

Accela will provide mirrored secondary site allows for replication of the primary site in the event of a natural disaster rendering the primary data center inoperable. Accela will provide skilled staff to support all operational support services. These services include support processes necessary to provide a secondary mirrored site.

S. Data Recovery

Accela will provide multiple ways to recover data:

> Suspected error conditions will be investigated and corrected by ACCELA personnel at ACCELA'S offices to the extent possible. Onsite corrections shall be at the exclusive judgement of ACCELA at no additional cost to the User. User may, however, request that ACCELA conduct such investigations and travel to the location of the User at the User's request; User will pay ACCELA for reasonable travel and subsistence expenses. If ACCELA, in its reasonable judgment, determines that the suspected error condition was attributable to a

cause other than an error in ACCELA'S Subscribed Service or an enhancement by ACCELA, the User will pay for ACCELA'S efforts on a time and materials basis.

ACCELA may provide the User with unsolicited error corrections or changes to the Subscribed Service, without additional charge, which ACCELA determines are necessary for proper operation of its Subscribed Service, and User shall incorporate these corrections or changes into the Subscribed Service within 180 days of release by ACCELA. ACCELA will provide all documentation changes necessary as a result of changes to the software.

ACCELA will provide User all enhancements released by ACCELA as standard enhancements, and which are generally made available to other users purchasing comparable Subscribed Service during the term of this Agreement.

EXHIBIT I
ATTACHMENT A

ACCELA, INC. SERVICE LEVEL COMMITMENT

This SaaS Service Level Commitment ("SLC") is a policy governing the use of Accela software-as-service products (individually or collectively, the "Service") under the terms of the Accela Master Services Agreement (the "Agreement") between Accela, Inc. and its affiliates ("Accela", "us" or "we") and the purchaser of Accela's Subscription Service ("Customer").

Unless otherwise provided herein, this SLC is subject to the terms of the Agreement and capitalized terms will have the meaning specified in the Agreement. Accela reserves the right to change the terms of this SLC in accordance with the Agreement.

DEFINITIONS

"Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which the Service was Unavailable. Measurement of the Monthly Uptime Percentage excludes downtime resulting directly or indirectly from any SLC Exclusion.

"Service Credit" is a dollar credit, calculated as set forth below, that Accela may credit back to an eligible Customer account.

"Unavailable" means, as applicable: (i) Customer is repeatedly unable to log into the Service; (ii) Customer experiences repeated connection request failures; (iii) Customer experiences lack of connectivity of external, public instances or sites lasting for more than five (5) minutes; (iv) Customer is unable to connect and sync mobile applications within the Service to Accela servers; and/or (v) Customer is unable to download or sync data from mobile applications within the Service to Accela servers. The foregoing events must be verifiable or replicable by Accela or its designee. Availability of Accela APIs, as separate from Service access, is expressly excluded from this SLC.

SERVICE COMMITMENT

Accela will use commercially reasonable efforts to make the Service available with a Monthly Uptime Percentage of at least 99.9%, in each calendar month of the Subscription Period (the "Commitment"). In the event the Service does not meet this Commitment, Customer will be eligible to receive a Service Credit as described below.

SCHEDULED & EMERGENCY MAINTENANCE

Accela will maintain certain scheduled maintenance windows during which regular, planned maintenance of the Service may be performed. Accela will use commercially reasonable efforts to provide Customer with no less than twenty-four (24) hours' notice prior to Services unavailability due to planned maintenance.. Accela's standard maintenance window will generally fall between the hours of 9:00 PM [21:00] Thursday and 1:00 AM [1:00] Friday local time.

Accela will endeavor to provide as much notice as is practicable under the circumstances for patches, updates, fixes and other emergency maintenance activities which may be applied on an urgent basis.

Accela will provide three (3) business days' notice prior to any planned network, server hardware, operating environment, or database modifications of a material nature.

SERVICE CREDITS

System availability is measured by the following formula:

$$x = (n - y) * 100 / n$$

Notes: (1) "x" is the uptime percentage; "n" is the total number of hours in the given calendar month minus scheduled downtime; and "y" is the total number of downtime hours in the given calendar month. (2) Specifically excluded from "n and "y" in this calculation are the exception times on scheduled upgrade and maintenance windows.

Service Availability	Percentage of Monthly Service Fees Credited
> 99.9%	2%
99.5% - < 99.9%	5%
99.0% - < 99.5%	10%
95.0% - < 99.0%	0%
90.0% - < 95.0%	40%
< 90.0% - < 80.0%	45%
< 80%	50%

Accela will apply any Service Credits only against future Service payments otherwise due from Customer. Service Credits will not entitle Customer to any refund or other payment from Accela. Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Agreement, Customer's sole and exclusive remedy for any unavailability, non-performance, or other failure by Accela to provide the Service is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLC.

SLC EXCLUSIONS

The Service Commitment does not apply to any unavailability, suspension or termination of the Service or any Service performance issues: (i) caused by factors outside of Accela's reasonable control, including any force majeure event or Internet access or related problems beyond the Service demarcation point; (ii) that result from customizations (if outside of Accela's best practice recommendations), configuration changes, scripting, or data loss caused by or on behalf of Customer or any End User; (iii) that result from Customer's or any End User's or third party's equipment, software or other technology or integrations (other than third party equipment within Accela's direct control); (iv) that result from any maintenance as provided for pursuant to the above terms; or (vii) arising from our suspension or termination of Customer's right to use the Service in accordance with the Agreement (collectively, the "SLC Exclusions"). If availability is impacted by factors other than those used in the Monthly Uptime Percentage calculation, Accela may issue a Service Credit with consideration to pertinent factors as assessed by Accela in its sole discretion.

SUPPORT COMMITMENT

This Silver Support SLA Addendum (the "Addendum") is issued under and subject to additional conditions and limitations as set out in the agreement by and between Accela and Customer.

The following Issues, Response Goals and Resolution Goals are applicable to support services for Accela supported products functioning in Customer's production environment (the "Supported Products") and is not applicable to any other Accela software, services or environments. Any references to "business day" are exclusive of the U.S. federal and state holidays observed by Accela:

Priority	Definition	Response Goal	Resolution Goal
Critical Severity Issue (Priority 1)	Supported Product is non-functional or seriously affected and there is no reasonable workaround available (e.g. business is halted).	Confirmation of receipt within one (1) business hour. Update as information arrives or at the interval specified by Customer.	Upon confirmation of receipt, Accela will put forth our best effort to provide a workaround, fix, or estimated completion date within seventy-two (72) hours after the problem has been diagnosed and/or replicated.
High Severity Issue (Priority 2)	Supported Product is affected and there is no workaround available or the workaround is impractical (e.g. Supported Product response is very slow, day to day operations continue but are impacted by the work around).	Confirmation of receipt within four (4) business hours.	Accela will put forth our best effort to provide a workaround or fix or estimated completion date within fourteen (14) business days after the problem has been diagnosed and/or replicated.
Medium Severity Issue (Priority 3)	Support Product is non-functional however a convenient workaround exists (e.g. non-critical feature is unavailable or requires additional user intervention).	Confirmation of receipt within eight (8) business hours.	Accela will put forth our best effort to provide a workaround or fix or estimated completion date within twenty-one (21) business days after the problem has been diagnosed and/or replicated.
Low Severity Issue (Priority 4)	Supported Product works, but there is a minor problem (e.g. incorrect label, or cosmetic defect).	Confirmation of receipt within twenty-four (24) business hours.	Resolution for the Issue may be released as a patch set or be incorporated into a future schedule release of the product.