County of Santa Clara

Office of the County Executive
Procurement Department
150 W. Tasman Drive, First Floor
San Jose, CA 95134
Telephone 408-491-7400 ● Fax 408-491-7496

FOURTH AMENDMENT TO AGREEMENT CW2226606 BY AND BETWEEN THE COUNTY OF SANTA CLARA AND TYLER TECHNOLOGIES, INC.

This is the Fourth Amendment to the Agreement between the County of Santa Clara (County) and Tyler Technologies, Inc. (Contractor) originally entered into on August 8, 2017, for the CivilServe and CivilMobile Client License for the County.

This Agreement is amended as follows, effective February 8, 2022:

1. Key Provision, **AGREEMENT TERM**, is revised to read: "This Agreement commences on August 8, 2017, and expires on August 7, 2027 with an option to renew for one additional two-year period."

2. Key Provision, **TOTAL AGREEMENT VALUE**, is revised to read: "The total not to exceed value of this Agreement is $822,425, which represents an increase of $283,361 from the prior not to exceed value of $539,064."

   Contractor understands that this not to exceed value does not represent a commitment by County to Contractor.

3. Add **EXHIBIT 2.4, TYLER'S SERVICES**, attached hereto and incorporated herein by this reference.

4. Add **EXHIBIT 7, CONTRACTOR CERTIFICATION OF COMPLIANCE WITH COVID-19 VACCINE REQUIREMENTS**, attached hereto and incorporated herein by this reference.

5. Add **EXHIBIT 8, REMOTE ACCESS**, attached hereto and incorporated herein by this reference.

6. Replace **EXHIBIT 5, COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES**, with **EXHIBIT 5.1, COUNTY IT USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES**, attached hereto and incorporated herein by this reference.

7. **EXHIBIT 1, COUNTY OF SANTA CLARA TERMS AND CONDITIONS**, is revised to add the following provisions:

   "**25. COVID-19 REQUIREMENTS**
   Contractor shall comply with all County requirements relating to COVID-19 for persons who routinely perform services for the County onsite and share airspace with or proximity to other people at a County facility as part of their services for the County, including but not limited to vaccination, as applicable and periodically updated, and available at https://procurement.sccgov.org/doing-business-county/contractor-vaccinations and incorporated herein by this reference. If applicable, Contractor shall complete the Contractor Certification of Compliance with COVID-19 Vaccine Requirements ("Certification"), attached hereto as Exhibit 7. Contractor shall comply with the requirements of this Section for the

entire term of this Agreement.

Contractor shall comply with all reasonable requests by County for documentation demonstrating Contractor's compliance with this Section. Failure by Contractor to comply with any of the requirements of this Section (including but not limited to vaccination and masking requirements and completion and submittal of the Certification) is a material breach of this Agreement, and the County may, in its sole discretion terminate this Agreement in accordance with the procedures set forth in Section 16.2 of Exhibit 2, Tyler Technologies License and Service Agreement.

26. CONTRACTOR TRAVEL EXPENSES
Contractor and County agree that there will be no travel or on-site services provided under this Agreement. Should the County require on-site services, the parties will enter into a written amendment to this Agreement to set forth the terms of such services.

27. CLICK-THROUGH AGREEMENTS AND CONTRACTOR POLICIES
(1) No provisions of any shrink-wrap or any click-through agreement (or other form of "click to accept" agreement) that may routinely accompany any products or services acquired under this Agreement shall apply in place of, or serve to modify any provision of this Agreement, even if a user or authorized officer of County purports to have affirmatively accepted such shrink-wrap or click through provisions. Without limiting the foregoing, no "terms of use," "privacy policy" or other policy on Contractor's website or application (collectively, "Policies") or another website that may routinely accompany any products or services acquired under this Agreement shall apply in place of or serve to modify any provision of this Agreement.

(2) For the avoidance of doubt and without limiting the foregoing, in the event of a conflict between any such shrink-wrap, click-through provisions or Policies (irrespective of the products or services that such provisions attach to) and any term or condition of this Agreement, the relevant term or condition of this Agreement shall govern to the extent of any such conflict. Only the provisions of this Agreement as amended from time to time, and executed by the parties, shall apply to County and or authorized user.

(3) The parties acknowledge that the County and or authorized users may be required to click "Accept" as a routine condition of access to services through the Contractor's website or other application. Such click-through provisions or Policies on Contractor's website shall be null and void for County and/or each such authorized user and shall only serve as a mechanical means for accessing such services."

8. Replace Subdivision (d), Equal Opportunity/Non-Discrimination, and Subdivision (g), Wage Theft, of **SECTION 19, COUNTY SPECIFIC TERMS**, in **EXHIBIT 1, COUNTY OF SANTA CLARA TERMS AND CONDITIONS,** in their entirety with the following:

   "(d) COMPLIANCE WITH ALL LAWS AND REGULATIONS INCLUDING NONDISCRIMINATION, EQUAL OPPORTUNITY, AND WAGE THEFT PREVENTION

   Contractor's violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the Agreement in accordance with the procedures set forth in Section 16.2 of Exhibit 2, Tyler Technologies License and Service Agreement. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 et seq. the Fair Packaging and Labeling Act. and the standards and regulations issued there under. Contractor agrees to indemnify and

hold harmless the County for any loss, damage, fine, penalty, or any expense whatsoever as a result of Contractor's failure to comply with the act and any standards or regulations issued there under. County must notify Contractor promptly in writing of any claim under this paragraph and give Contractor sole control over its defense or settlement, except to the extent the defense or settlement purport to bind the County or find fault lies with the County.

(1) Compliance with All Laws. Contractor shall comply with all applicable Federal, State, and local laws, regulations, rules, and policies (collectively, "Laws"), including but not limited to the non-discrimination, equal opportunity, and wage and hour Laws referenced in the paragraphs below.

(2) Compliance with Non-Discrimination and Equal Opportunity Laws: Contractor shall comply with all applicable Laws concerning nondiscrimination and equal opportunity in employment and contracting, including but not limited to the following: Santa Clara County's policies for contractors on nondiscrimination and equal opportunity; Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; the Age Discrimination in Employment Act of 1967; the Rehabilitation Act of 1973 (Sections 503 and 504); the Equal Pay Act of 1963; California Fair Employment and Housing Act (Government Code sections 12900 et seq.); California Labor Code sections 1101, 1102, and 1197.5; and the Genetic Information Nondiscrimination Act of 2008. In addition to the foregoing, Contractor shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political belief, organizational affiliation, or marital status in the recruitment, selection for training (including but not limited to apprenticeship), hiring, employment, assignment, promotion, layoff, rates of pay or other forms of compensation. Nor shall Contractor discriminate in the provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex, gender identity, gender expression, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.

(3) Compliance with Wage and Hour Laws: Contractor shall comply with all applicable wage and hour Laws, which may include but are not limited to, the Federal Fair Labor Standards Act, the California Labor Code, and, if applicable, any local Minimum Wage, Prevailing Wage, or Living Wage laws.

(4) Definitions: For purposes of this Section, the following definitions shall apply. A "Final Judgment, Decision, Determination, or Order" shall mean a judgment, decision, determination, or order (a) which is issued by a court of law, an investigatory government agency authorized by law to enforce an applicable Law, an arbiter, or arbitration panel and (b) for which all appeals have been exhausted or the time period to appeal has expired. For pay equity Laws, relevant investigatory government agencies include the federal Equal Employment Opportunity Commission, the California Division of Labor Standards Enforcement, and the California Department of Fair Employment and Housing. Violation of a pay equity Law shall mean unlawful discrimination in compensation on the basis of an individual's sex, gender, gender identity, gender expression, sexual orientation, race, color, ethnicity, or national origin under Title VII of the Civil Rights Act of 1964 as amended, the Equal Pay Act of 1963, California Fair Employment and Housing Act, or California Labor Code section 1197.5, as applicable. For wage and hour Laws, relevant investigatory government agencies include the federal Department of Labor, the California Division of

Labor Standards Enforcement, and the City of San Jose's Office of Equality Assurance.

(5) Prior Judgments, Decisions or Orders against Contractor: By signing this Agreement, Contractor affirms that it has disclosed any final judgments, decisions, determinations, or orders that (a) were issued in the five years prior to executing this Agreement by a court or investigatory government agency and (b) found that Contractor violated an applicable wage and hour or pay equity law. Contractor further affirms that it has satisfied and complied with – or has reached agreement with the County regarding the manner in which it will satisfy – any such final judgments, decisions, determinations, or orders.

(6) Violations of Wage and Hour Laws or Pay Equity Laws During Term of Agreement: If at any time during the term of this Agreement, Contractor receives a Final Judgment, Decision, Determination, or Order rendered against it for violation of an applicable wage and hour Law or pay equity Law, then Contractor shall promptly satisfy and comply with any such Final Judgment, Decision, Determination or Order. Contractor shall inform the Office of the County Executive-Office of Countywide Contracting Management (OCCM) of any relevant Final Judgment, Decision, Determination, or Order against it within 30 days of the Final Judgment, Decision, Determination, or Order becoming final or of learning of the Final Judgment, Decision, Determination, or Order, whichever is later. Contractor shall also provide any documentary evidence of compliance with the Final Judgment, Decision, Determination, or Order within 5 days of satisfying the Final Judgment, Decision, Determination, or Order. Any notice required by this paragraph shall be addressed to the Office of the County Executive-OCCM at 70 W. Hedding Street, East Wing, 11th Floor, San José, CA 95110. Notice provisions in this paragraph are separate from any other notice provisions in this Agreement and, accordingly, only notice provided to the Office of the County Executive-OCCM satisfies the notice requirements in this paragraph.

(7) Access to Records Concerning Compliance with Pay Equity Laws: In addition to and notwithstanding any other provision of this Agreement concerning access to Contractor's records, Contractor shall permit the County and/or its authorized representatives to audit and review records related to compliance with applicable pay equity Laws. Upon the County's request, Contractor shall provide the County with access to any records, including but not limited to financial and employee records, that are related to the purpose of this Section, except where prohibited by federal or state laws, regulations or rules. County's access to such records shall be permitted at any time during Contractor's normal business hours upon no less than 10 business days' advance notice.

(9) Material Breach: Failure to comply with any part of this Section shall constitute a material breach of this Agreement. In the event of such a breach, the County may, in its discretion, exercise any or all remedies available under this Agreement and/or at law. County may, among other things, take any or all of the following actions:

(i) Suspend or terminate any or all parts of this Agreement, in accordance with the procedures set forth in Section 16.2 of Exhibit 2, Tyler Technologies License and Service Agreement.
(ii) Withhold payment to Contractor until full satisfaction of a Final Judgment, Decision, Determination, or Order.
(iii) Offer Contractor an opportunity to cure the breach.

(10) Subcontractors: Contractor shall impose all of the requirements set forth in this Section on any subcontractors permitted to perform work under this Agreement. This includes

ensuring that any subcontractor receiving a Final Judgment, Decision, Determination, or Order for violation of an applicable wage and hour Law promptly satisfies and complies with such Final Judgment, Decision, Determination, or Order."

9. Replace Section 17, Dispute Resolution, of **EXHIBIT A, SOFTWARE LICENSE AND PROFESSIONAL SERVICES AGREEMENT,** in its entirety with the following:

   Disputes arising out of, or relating to, this Agreement shall first be discussed by the Project Managers. Any dispute that cannot be resolved within five (5) Business Days at the Project Manager level (or such other date as agreed upon by the Project Managers) shall be referred to the individual reasonably designated by Purchaser and Tyler's Vice President of Courts and Justice Systems Division assigned to Purchaser's account ("Intermediary Dispute Level"). Any dispute that cannot be resolved in ten (10) Business Days at the Intermediary Dispute Level shall then be referred to Purchaser's chief executive officer or other individual reasonably designated by Purchaser and Tyler's President of Courts and Justice Systems Division ("Executive Dispute Level"), at such time and location reasonably designated by the Parties. Subject to the applicable provisions of the California Public Records Act and Section 9(f) of Exhibit 1 of the Agreement, any negotiations pursuant to this Section 17 are confidential and shall be treated as compromise and settlement negotiations for purposes of the applicable rules of evidence. The foregoing shall not apply to claims for equitable relief under Section 9 of this Exhibit.

All other terms and conditions of the Agreement, as amended, remain in full force and effect. In the event of a conflict between the original Agreement, as amended, and this Amendment, this Amendment controls.

By signing below, signatory warrants and represents that he/she executed this Amendment in his/her authorized capacity, that he/she has the authority to bind the entity listed below to contractual obligations and that by his/her signature on this Amendment, the entity on behalf of which he/she acted, executed this Amendment.

COUNTY OF SANTA CLARA

DocuSigned by:
Scott Zimmer
F491A917015540D6...
2/9/2023
For: Director of Procurement Date

APPROVED AS TO FORM AND LEGALITY

DocuSigned by:
Tara Lundstrom
D1B63BA915E8478...
2/8/2023
Tara Lundstrom Date
Deputy County Counsel

CONTRACTOR

By: DocuSigned by:
Sherry Clark
649203B6339141C...

Print: Sherry Clark

Title: Group General Counsel

Date: 2/8/2023

Attachments:
Exhibit 2.1, Tyler's Services
Exhibit 5.1, County IT User Responsibility Statement for Third Parties

Exhibit 7, Contractor Certification of Compliance with Covid-19 Vaccine Requirements
Exhibit 8, Remote Access

EXHIBIT 2.4
TYLER'S SERVICES

Investment Summary

Maintenance & Support					
	Year 6	**Year 7**	**Year 8**	**Year 9**	**Year 10**
Software	**8/8/2022 – 8/7/2023**	**8/8/2023 – 8/7/2024**	**8/8/2024 – 8/7/2025**	**8/8/2025 – 8/7/2026**	**8/8/2026 – 8/7/2027**
CivilServe Annual Support	$47,129.60	$49,957.38	$52,954.82	$56,661.66	$60,627.97
CivilMobile Annual Support	$6,204.90	$6,577.19	$6,971.83	$7,459.85	$7,982.04
Escrow – Annual Beneficiary Fee	$1,500	$1,500	$1,500	$1,500	$1,500
Amount Previously Invoiced	($26,667.19)				
Totals					
Total Annual Maintenance &Support Due, including Escrow	$28,167.27	$58,034.57	$61,426.65	$65,621.51	$70,110.01
				GRAND TOTAL	**$283,360.01**

EXHIBIT 7
CONTRACTOR CERTIFICATION OF COMPLIANCE WITH COVID-19 VACCINE REQUIREMENTS
(Version Effective September 27, 2022)

Contractor Information:

Contractor name:	Name of Contractor representative:
Tyler Technologies, Inc.	Sherry Clark
Contractor phone number:	Contractor email address:
972-713-3770	Sherry.Clark@tylertech.com

Contractor Certification. On behalf of Contractor, I hereby certify that:

1. Contractor has reviewed and is in compliance with all current County requirements regarding COVID-19 vaccination applicable to contractor's personnel working at County facilities, including but not limited to the requirements in the County's memorandum regarding COVID-19 Vaccine Requirement for County Personnel ("County Vaccine Policy"), the County's memorandum regarding Application of COVID-19 Vaccination Requirement to County Contractors, Interns, and Volunteers, all current State and County Health Officer orders, and any other County requirements. These memoranda and current County policies are accessible at <https://procurement.sccgov.org/doing-business-county/contractor-vaccinations>. Contractor understands that it is responsible for reviewing and maintaining compliance with all subsequent revisions or amendments to State and County orders and requirements regarding COVID-19.

2. As of the date signed below:

    a. Contractor understands that it must confirm, and has confirmed, that all of contractor's personnel (including any subcontractor personnel) who routinely perform services for the County onsite and share airspace with or proximity to other people at an indoor County facility as part of their services for the County[1] are:

        i. Fully vaccinated against COVID-19 as defined and required in the County Vaccine Policy;[2] **or**

        ii. Have a legally sufficient and approved medical, disability, or religious exemption from vaccination that has been granted by contractor.

[1] As established in the County's Memorandum Regarding Application of COVID-19 Vaccination Requirement to County Contractors, Interns, and Volunteers, contractors performing work at closed construction sites are not required to comply with the County's vaccination requirements, but must comply with all applicable federal, state, and local public health laws, including but not limited to any vaccination, testing, and masking requirements.

[2] County departments are required by law to implement any State-issued requirements, including ones that are more restrictive than the County's internal policies. As of the date of this policy, the California Department of Public Health (CDPH) requires that workers in health care facilities, as well as specified workers in custodial settings, obtain a COVID- 19 booster dose. Thus, contractor personnel subject to this CDPH booster requirement are expected to comply with it, in addition to the County's policy. The exemption process in Section C of the County Vaccine Policy shall apply to any requests for exemption from the State booster requirement.

b. Contractor has verified and will continue to verify the vaccination status of all staff working on site at any County facility, and has obtained proof of vaccination from its staff in a form consistent with the California Department of Public Health's Vaccine Records Guidelines and Standards.

3. If contractor seeks to send any personnel who are not fully vaccinated to work indoors at any County facility because the contractor has granted them an exemption, contractor shall notify the County in writing by providing a list of any such personnel to the COVID-19 Designee for the department that manages the facility where the contractor personnel will be working at least 96 hours in advance of any such personnel arriving onsite so that the department has sufficient time to determine whether it will approve the contractor's requests that its personnel work onsite and, if approved, can ensure that the contractor has complied with all applicable COVID-19 safety requirements for unvaccinated individuals, including, where appliable, regular testing and the use of a fit-tested N95 mask.[3] Notice must be separately provided to each department that manages a facility where contractor seeks to assign personnel to work onsite.

4. If any of contractor's personnel are noncompliant with vaccination or testing requirements, contractor will notify the County Department for which they are providing services immediately and will not permit those personnel to go onsite at a County facility without express written permission from the County.

5. Contractor will comply with all reasonable requests by the County for documentation demonstrating the contractor's compliance with this Certification.

I verify the truth and accuracy of the statements in this Certification under penalty of perjury under thelaws of the State of California.

Sherry Clark	Group General Counsel
Name of authorized representative of Contractor	Title
DocuSigned by: Sherry Clark 649203B6339141C...	2/8/2023
Signature	Date

[3] If contractor sends personnel who are not fully vaccinated, it is contractor's obligation to ensure that it has any necessary authorization under the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 et. seq., and under any other laws to share this information with the County

.

EXHIBIT 8
REMOTE ACCESS

1. Definitions

(a) "Remote Access" is the act of accessing County Systems from a non-County network infrastructure.

(b) "County Systems," for purposes of this Exhibit, include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data, except for Contractor-owned systems, applications, software and the like that process County information/data in performing Contractor's obligations under this Agreement. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

(c) "County-owned information/data," for purposes of this Exhibit, is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.

(d) "Contractor employees" includes Contractor's employees, agents, representatives, contractors or subcontractors performing services under this Agreement.

2. Scope of Access

(a) County grants Remote Access privileges (through the method described in section 9) for Contractor to access the following County Systems (collectively referred to as "Designated Systems"), in accordance with the terms of this Agreement:

All Tyler applications licensed by the County under the Agreement.

(b) All other forms of access to the Designated Systems, or to any County System that is not specifically named, is prohibited.

(c) Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in this Agreement including, but not limited to, supporting Contractor-installed programs. Any access to the Designated Systems, County-owned information/data, or any other County System or asset that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of this Agreement for cause and any penalty allowed by law. Contractor may only access the

Designated Systems; provided, however, that if access to other County Systems is necessary for Contractor to provide services and perform its obligations under this Agreement, Contractor shall be authorized to access such County Systems for such limited purpose.

(d) County will review the scope of Contractor's Remote Access rights periodically.

3. Security Requirements

(a) Contractor will not install any Remote Access capabilities on any County System unless such installation and configuration is approved by the County Information Security Office and meets relevant NIST 800-53 standards, or an equivalent industry standard. Approval will be deemed given if and when a remote access session is initiated or accepted by County personnel.

(b) Contractor will only remotely access Designated Systems, including access initiated from a County System, if the following conditions are met:

(i) The Remote Access method agreed upon pursuant to paragraph 9 must include the following minimum control mechanisms:

(aa) Two-Factor Authentication: An authentication method that requires the following factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., an email address at which the County will send a unique security code); and 2) something you know (e.g., a password).

(bb) County personnel will control authorizations (permissions) to specific systems or networks.

(cc) All Contractor systems used to remotely access County Systems must have industry-standard anti-virus and other security measures (e.g., software firewall) installed, configured, and activated.

4. Monitoring/Audit

County will monitor access to, and activities on, County Systems, including all Remote Access attempts. Data on all activities will be logged on a County System and will include the date, time, and user identification.

5. Copying, Deleting or Modifying Data

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County System unless otherwise stated in this Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in this Agreement. Contractor may copy data during a support session in order to properly triage an issue if it receives oral approval from County personnel during that session.

6. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect data contained on County Systems within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County Systems from a non-designated system. Such access will use information security protocols that meet relevant NIST 800-53 standards, or an equivalent industry standard. Remote Access must include the control mechanisms noted in Paragraph 3(b)(ii) above.

7. Remote Access Contacts

The following persons are points of contact for purposes of this Exhibit:

Contractor: Jake Ross, Software Support Manager
Phone: 774.348.3000 ext: 713003
Email: jake.ross@tylertech.com

County: **Vincent Poon, IT Project Manager**
Phone: 408-808-4610
Email: Vincent.Poon@shf.sccgov.org

Either party may change the aforementioned names by providing the other party with no less than three (3) business days prior written notice.

8. Additional Requirements

Contractor agrees to the following:

(a) Only Contractor employees providing services or fulfilling Contractor obligations under this Agreement will be given Remote Access rights.

(b) Any access to Designated Systems, other County Systems and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in termination of the Agreement for cause and any other penalty allowed by law.

(c) An encryption method that meets Federal Information Processing Standard (FIPS) Publication 140-2 will be used.

(d) Contractor shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources.

(e) Contractor shall ensure compliance with the terms of this Exhibit and the Exhibit on County Information Technology User Responsibility Statement for Third Parties by all Contractor employees performing services under this Agreement.

(f) Contractor employees have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

(g) Contractor employees that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Contractor employees shall report loss or theft of such devices to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

9. Remote Access Methods

(a) All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County. The remote access solution must conform to County policy and security requirements.

(b) Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.

(c) Contractor agrees to abide by the following remote access method:

County-Controlled SecureLinkAccess ◉ **Primary** ○ **Backup** ○ **N/A**

This County-Controlled method involves using the Securelink tool installed in the County. County will establish a gateway where Contractor can access the Designated Systems from selected network-attached devices at the County site. County will control the access list for Contractors with access through SecureLink gateways.

EXHIBIT 9
COUNTY IT USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES

1. DEFINITIONS

(a) *"County Confidential Information"* is all material non-public information, written or oral, disclosed, directly or indirectly, through any means of communication or observation by County to Contractor or any of its affiliates or representatives

(b) *"County Systems"* include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data, except for Contractor-owned systems, applications, software and the like that process County information/data in performing Contractor's obligations under this Agreement. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

(c) "County-owned information/data," for purposes of this Exhibit is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.

(d) *"Mobile Device"* is any portable computing device that fits one of the following categories: laptops, smartphones, or tablets. "Mobile Device" does not include devices that are used exclusively for the purpose of making telephone calls.

(e) *"Users"* include all employees, agents and/or representatives of Contractor performing services under this Agreement.

2. GENERAL REQUIREMENTS

(a) Contractor will provide Users with a written copy of this Exhibit and will ensure that Users know, understand and comply with the requirements of this Exhibit. In all cases, such access shall be subject to approval by an authorized County representative.

(b) Users are personally responsible for knowing and understanding these requirements, and are personally responsible for any actions they take that do not comply with this Agreement. If a User is unclear as to requirements, User shall ask County for guidance.

(c) If a User is issued an account for a County System, User shall comply with the following County standards for password definition, use, and management for remote access to County systems via SecureLink:

(i) Minimum password length is 12 characters unless a particular County System has a different requirement or is not technically feasible.
(ii) The password must be high complexity (contains one of each, upper, lower, number, symbol).
(iii) The password must be rotated every 90 days.
(iv) User must not reuse the last 10 passwords.
(v) Access to County System is denied after 5 failed logon attempts.

(d) Only authorized County staff may attach any form of computer equipment to a County network or system. This includes, but is not limited to, attachment of such devices as mobile devices, peripherals (e.g., external hard drives, printers), and USB storage media. It excludes County wireless networks provided specifically for the use of guests or visitors to County facilities.

(e) User shall not use USB storage media on any County System. All such devices shall be County-owned, formally issued to User by County, and used only for legitimate County purposes.

(f) User shall not connect County-owned computing equipment, including USB storage media, to non-County systems or networks, unless County gives its express written permission. This formal approval process ensures that the non-County system or network in question has been evaluated for compliance with County security standards. An example of a permitted connection to a non-County system or network would be approved connection of a County issued laptop to a home network.

(g) User shall not install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County System, without County's express written permission. If authorized to install, configure or use such a device, User shall comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County Systems. Any allowed installation shall not be activated until it is reviewed and approved in writing by an authorized County representative.

(h) The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.

(i) Users shall not attempt to elevate or enhance their assigned level of privileges unless County gives its express written permission. Users who have been granted enhanced privileges due to their specific roles, such as system or network administrators, shall not abuse these privileges and shall use such privileges only in the performance of appropriate, services performed under this Agreement.

(j) Users shall use County-approved authentication mechanisms when accessing County networks and systems, and shall not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by County.

(k) Users shall not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or installed, it is the responsibility of the User to check with County.

(l) All software on County Systems shall be installed by authorized County support staff except as provided in this Agreement. Users may not download or install software on any County system unless express written permission has been obtained from County such as in this Agreement.

(m) Users shall immediately report to the County TechLink Center the loss or theft of County-owned computer equipment, or of personally-owned computer equipment that contains County Data. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org.

(n) Users shall respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:

(i) Users shall not access, or attempt to access, County Systems or County-owned information/data unless specifically authorized to do so by the terms of this Agreement or in the performance of its obligations under this Agreement.

(ii) If User is assigned a County account, User shall not allow unauthorized individuals to use their account; this includes the sharing of account passwords.

(iii) Users shall not without County's written permission, use or disclose County-owned information/data other than in the performance of its obligations under this Agreement.

(iv) Users shall take every precaution to ensure that all confidential or restricted information is protected from disclosure to unauthorized individuals.

(v) Users shall not make or store paper or electronic copies of information unless required to provide services under this Agreement.

(vi) Users shall comply with all confidentiality requirements in Contractor's Agreement with the County. Users shall not use or disclose County Confidential Information other than in the performance of its obligations for County. All County Confidential Information shall remain the property of the County. User shall not acquire any ownership interest in County Confidential Information.

(o) Users shall do all of the following:

(i) Users shall not change or delete County-owned information/data unless performing such changes is required to perform services under this Agreement.

(ii) Users shall avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.

(iii) Upon termination or expiration of this Agreement, Users shall not retain, give away, or remove any County-owned information/data or document from any County System or County premises. Users shall return to County all County-owned assets, including hardware and data.

(p) Electronic information transported across any County network, or residing in any County System, is potentially subject to access by County technical support staff, other County personnel, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County System.

(q) Users must protect, respect and not infringe upon all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, County Confidential Information, and confidential information belonging to any other third party.

(r) All information resources on any County System are the property of County and are therefore subject to County policies regarding acceptable use. No User may use any County System or County-owned information/data for the following purposes:

(i) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization that are not related to the User conducting County business. This prohibition does not apply to User's performance of contractual obligations for the County.

(ii) Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.

(iii) To access, create, transmit, print, download or solicit material that is, or may be construed to be, harassing or demeaning toward any individual or group for any reason, including but not limited to on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business.

(iv) To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business.

(v) Knowingly propagating or downloading viruses or other malicious software.

(vi) Disseminating hoaxes, chain letters, or advertisements.

3. INTERNET AND EMAIL

(a) Users shall not use County Systems for personal activities.

(b) When using a County-owned device to conduct County business or perform services under this Agreement, Users shall not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by County. Such services include, but are not limited to, file sharing (such as Dropbox, Box, Google OneDrive), Instant Messaging (such as AOL IM), email services (such as Hotmail and Gmail), peer-to-peer networking services (such as Kazaa), and social networking services (such as blogs, Instagram, Snapchat, MySpace, Facebook and Twitter). If a User has received express written permission to access such services from a County-owned device, User shall comply with all relevant County policies, procedures, and guidelines.

4. REMOTE ACCESS

(a) Users are not permitted to implement, configure, or use any remote access mechanism unless the County has authorized the remote access mechanism.

(b) County may monitor and/or record remote access sessions, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

(c) User shall configure all computer devices used to access County resources from a remote location according to relevant NIST 800-53 standards, or an equivalent industry standard. These include anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other relevant security software or security-related system configurations.

(d) Users that have been physically provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Users shall immediately report loss or theft of such devices to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.

(e) Users shall comply with any additional remote access requirements in this Agreement such as an Exhibit on Remote Access.

5. THIRD PARTY-OWNED DEVICES

(a) This Section 5 applies if County permits Users to perform services under this Agreement with devices not owned by the County ("Third-party owned device"). Third-party owned devices include devices with email and/or data storage capability (such as laptops, iPhones, iPads, Android phones and tablets, BlackBerry and other "smart" devices).

(b) The third party-owned device in question shall use County-approved access/authentication systems when accessing County Systems. Approval will be deemed given if and when a Remote Access session is initiated or accepted by County personnel.

(c) Users shall adhere to all relevant security policies and standards as mutually agreed to by County and Contractor in this Agreement.

(d) Users shall treat the County-owned communications, information or files the third-party owned device contains as County property. User shall not allow access to or use of any County-owned communications, information, or files by individuals who have not been authorized by County to access or use that data.

(e) To the extent that County-owned data/information is contained on the third-party owned device, Users shall report the loss or theft of the device immediately to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.