Agreement No. _____

AGREEMENT BETWEEN THE COUNTY OF SAN MATEO AND INTERPERSONAL FREQUENCY, LLC

This Agreement is entered into this _____ day of _____, 20_____, by and between the County of San Mateo, a political subdivision of the state of California, hereinafter called "County," and, hereinafter called "Contractor."

* * *

Whereas, pursuant to Section 31000 of the California Government Code, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof; and

Whereas, it is necessary and desirable that Contractor be retained for the purpose of providing managed Drupal website maintenance, development, and hosting services for the County's Drupal website and content management system.

Now, therefore, it is agreed by the parties to this Agreement as follows:

1. Exhibits and Attachments

The following exhibits and attachments are attached to this Agreement and incorporated into this Agreement by this reference:

Exhibit A—Services
Exhibit B—Payments and Rates
Exhibit C – Fulcrum and Voice of Citizen-Patron SaaS Services Agreement Spring 2021
Exhibit D – Premier Service Level Agreement; Support & Maintenance Terms
Exhibit E – Terms of Service for Voice of Citizen® and/or Voice of Patron® SaaS
Attachment H—HIPAA Business Associate Requirements
Attachment IP – Intellectual Property

To the extent that any terms of the exhibits or attachments conflict with this Agreement, the terms of this Agreement shall control.

2. Services to be performed by Contractor

In consideration of the payments set forth in this Agreement and in Exhibit B, Contractor shall perform services for County in accordance with the terms, conditions, and specifications set forth in this Agreement and in Exhibit A.

3. Payments

In consideration of the services provided by Contractor in accordance with all terms, conditions, and specifications set forth in this Agreement and in Exhibit A, County shall make payment to Contractor based on the rates and in the manner specified in Exhibit B. County reserves the right to withhold payment if County determines that the quantity or quality of the work performed

is unacceptable. In no event shall County's total fiscal obligation under this Agreement exceed Six Hundred Forty-Nine Thousand, One Hundred Eighteen Dollars and Sixty-Seven Cents ($649,118.67). In the event that the County makes any advance payments, Contractor agrees to refund any amounts in excess of the amount owed by the County at the time of contract termination or expiration. Contractor is not entitled to payment for work not performed as required by this agreement.

4. Term

Subject to compliance with all terms and conditions, the term of this Agreement shall be from October 18, 2022, through October 17, 2025.

5. Termination

This Agreement may be terminated by Contractor or by the County's Information Services Department's (ISD) Chief Information Officer (CIO) or his/her designee at any time without a requirement of good cause upon thirty (30) days' advance written notice to the other party. Subject to availability of funding, Contractor shall be entitled to receive payment for work/services provided prior to termination of the Agreement. Such payment shall be that prorated portion of the full payment determined by comparing the work/services actually completed to the work/services required by the Agreement.

County may terminate this Agreement or a portion of the services referenced in the Attachments and Exhibits based upon the unavailability of Federal, State, or County funds by providing written notice to Contractor as soon as is reasonably possible after County learns of said unavailability of outside funding.

County may terminate this Agreement for cause. In order to terminate for cause, County must first give Contractor notice of the alleged breach. Contractor shall have five business days after receipt of such notice to respond and a total of ten calendar days after receipt of such notice to cure the alleged breach. If Contractor fails to cure the breach within this period, County may immediately terminate this Agreement without further action. The option available in this paragraph is separate from the ability to terminate without cause with appropriate notice described above. In the event that County provides notice of an alleged breach pursuant to this section, County may, in extreme circumstances, immediately suspend performance of services and payment under this Agreement pending the resolution of the process described in this paragraph. County has sole discretion to determine what constitutes an extreme circumstance for purposes of this paragraph, and County shall use reasonable judgment in making that determination.

6. Contract Materials

At the end of this Agreement, or in the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other written materials (collectively referred to as "contract materials") prepared by Contractor under this Agreement shall become

the property of County and shall be promptly delivered to County. Upon termination, Contractor may make and retain a copy of such contract materials if permitted by law.

7. Relationship of Parties

Contractor agrees and understands that the work/services performed under this Agreement are performed as an independent contractor and not as an employee of County and that neither Contractor nor its employees acquire any of the rights, privileges, powers, or advantages of County employees.

8. Hold Harmless

a. General Hold Harmless

Contractor shall indemnify and save harmless County and its officers, agents, employees, and servants from all claims, suits, or actions of every name, kind, and description resulting from this Agreement, the performance of any work or services required of Contractor under this Agreement, or payments made pursuant to this Agreement brought for, or on account of, any of the following:

(A) injuries to or death of any person, including Contractor or its employees/officers/agents;

(B) damage to any property of any kind whatsoever and to whomsoever belonging;

(C) any sanctions, penalties, or claims of damages resulting from Contractor's failure to comply, if applicable, with the requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all Federal regulations promulgated thereunder, as amended; or

(D) any other loss or cost, including but not limited to that caused by the concurrent active or passive negligence of County and/or its officers, agents, employees, or servants. However, Contractor's duty to indemnify and save harmless under this Section shall not apply to injuries or damage for which County has been found in a court of competent jurisdiction to be solely liable by reason of its own negligence or willful misconduct.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

b. Intellectual Property Indemnification

Contractor hereby certifies that it owns, controls, and/or licenses and retains all right, title, and/or interest in and to any intellectual property it uses in relation to this Agreement, including the design, look, feel, features, source code, content, and/or other technology relating to any part of the services it provides under this Agreement and including all related patents, inventions, trademarks, and copyrights, all applications therefor, and all trade names, service marks, know how, and trade secrets (collectively referred to as "IP Rights") except as otherwise noted by this Agreement.

Contractor warrants that the services it provides under this Agreement do not infringe, violate, trespass, or constitute the unauthorized use or misappropriation of any IP Rights of any third party. Contractor shall defend, indemnify, and hold harmless County from and against all liabilities, costs, damages, losses, and expenses (including reasonable attorney fees) arising out of or related to any claim by a third party that the services provided under this Agreement infringe or violate any third-party's IP Rights provided any such right is enforceable in the United States. Contractor's duty to defend, indemnify, and hold harmless under this Section applies only provided that: (a) County notifies Contractor promptly in writing of any notice of any such third-party claim; (b) County cooperates with Contractor, at Contractor's expense, in all reasonable respects in connection with the investigation and defense of any such third-party claim; (c) Contractor retains sole control of the defense of any action on any such claim and all negotiations for its settlement or compromise (provided Contractor shall not have the right to settle any criminal action, suit, or proceeding without County's prior written consent, not to be unreasonably withheld, and provided further that any settlement permitted under this Section shall not impose any financial or other obligation on County, impair any right of County, or contain any stipulation, admission, or acknowledgement of wrongdoing on the part of County without County's prior written consent, not to be unreasonably withheld); and (d) should services under this Agreement become, or in Contractor's opinion be likely to become, the subject of such a claim, or in the event such a third party claim or threatened claim causes County's reasonable use of the services under this Agreement to be seriously endangered or disrupted, Contractor shall, at Contractor's option and expense, either: (i) procure for County the right to continue using the services without infringement or (ii) replace or modify the services so that they become non-infringing but remain functionally equivalent.

Notwithstanding anything in this Section to the contrary, Contractor will have no obligation or liability to County under this Section to the extent any otherwise covered claim is based upon: (a) any aspects of the services under this Agreement which have been modified by or for County (other than modification performed by, or at the direction of, Contractor) in such a way as to cause the alleged infringement at issue; and/or (b) any aspects of the services under this Agreement which have been used by County in a manner prohibited by this Agreement.

The duty of Contractor to indemnify and save harmless as set forth by this Section shall include the duty to defend as set forth in Section 2778 of the California Civil Code.

9. Assignability and Subcontracting

Contractor shall not assign this Agreement or any portion of it to a third party or subcontract with a third party to provide services required by Contractor under this Agreement without the prior written consent of County. Any such assignment or subcontract without County's prior written consent shall give County the right to automatically and immediately terminate this Agreement without penalty or advance notice.

10. Insurance

a. General Requirements

Contractor shall not commence work or be required to commence work under this Agreement unless and until all insurance required under this Section has been obtained and such insurance has been approved by County's Risk Management, and Contractor shall use diligence to obtain such insurance and to obtain such approval. Contractor shall furnish County with certificates of insurance evidencing the required coverage, and there shall be a specific contractual liability endorsement extending Contractor's coverage to include the contractual liability assumed by Contractor pursuant to this Agreement. These certificates shall specify or be endorsed to provide that thirty (30) days' notice must be given, in writing, to County of any pending change in the limits of liability or of any cancellation or modification of the policy.

b. Workers' Compensation and Employer's Liability Insurance

Contractor shall have in effect during the entire term of this Agreement workers' compensation and employer's liability insurance providing full statutory coverage. In signing this Agreement, Contractor certifies, as required by Section 1861 of the California Labor Code, that (a) it is aware of the provisions of Section 3700 of the California Labor Code, which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of the Labor Code, and (b) it will comply with such provisions before commencing the performance of work under this Agreement.

c. Liability Insurance

Contractor shall take out and maintain during the term of this Agreement such bodily injury liability and property damage liability insurance as shall protect Contractor and all of its employees/officers/agents while performing work covered by this Agreement from any and all claims for damages for bodily injury, including accidental death, as well as any and all claims for property damage which may arise from Contractor's operations under this Agreement, whether such operations be by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or an agent of either of them. Such insurance shall be combined single limit bodily injury and property damage for each occurrence and shall not be less than the amounts specified below:

(a) Comprehensive General Liability……$1,000,000

(b) Motor Vehicle Liability Insurance……$1,000,000

(c) Professional Liability……$1,000,000

County and its officers, agents, employees, and servants shall be named as additional insured on any such policies of insurance, which shall also contain a provision that (a) the insurance afforded thereby to County and its officers, agents, employees, and servants shall be primary insurance to the full limits of liability of the policy and (b) if the County or its officers, agents, employees, and servants have other insurance against the loss covered by such a policy, such other insurance shall be excess insurance only.

In the event of the breach of any provision of this Section, or in the event any notice is received which indicates any required insurance coverage will be diminished or canceled, County, at its option, may, notwithstanding any other provision of this Agreement to the contrary, immediately declare a material breach of this Agreement and suspend all further work and payment pursuant to this Agreement.

11. Compliance With Laws

All services to be performed by Contractor pursuant to this Agreement shall be performed in accordance with all applicable Federal, State, County, and municipal laws, ordinances, and regulations, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Regulations promulgated thereunder, as amended (if applicable), the Business Associate requirements set forth in Attachment H (if attached), the Americans with Disabilities Act of 1990, as amended, and Section 504 of the Rehabilitation Act of 1973, which prohibits discrimination on the basis of disability in programs and activities receiving any Federal or County financial assistance. Such services shall also be performed in accordance with all applicable ordinances and regulations, including but not limited to appropriate licensure, certification regulations, provisions pertaining to confidentiality of records, and applicable quality assurance regulations. In the event of a conflict between the terms of this Agreement and any applicable State, Federal, County, or municipal law or regulation, the requirements of the applicable law or regulation will take precedence over the requirements set forth in this Agreement.

Contractor will timely and accurately complete, sign, and submit all necessary documentation of compliance.

12. Non-Discrimination and Other Requirements

a. General Non-discrimination

No person shall be denied any services provided pursuant to this Agreement (except as limited by the scope of services) on the grounds of race, color, national origin, ancestry, age, disability (physical or mental), sex, sexual orientation, gender identity, marital or domestic partner status, religion, political beliefs or affiliation, familial or parental status (including pregnancy), medical condition (cancer-related), military service, or genetic information.

b. Equal Employment Opportunity

Contractor shall ensure equal employment opportunity based on objective standards of recruitment, classification, selection, promotion, compensation, performance evaluation, and management relations for all employees under this Agreement. Contractor's equal employment policies shall be made available to County upon request.

c. Section 504 of the Rehabilitation Act of 1973

Contractor shall comply with Section 504 of the Rehabilitation Act of 1973, as amended, which provides that no otherwise qualified individual with a disability shall, solely by reason of a disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination in the performance of any services this Agreement. This Section applies only to contractors who are providing services to members of the public under this Agreement.

d. Compliance with County's Equal Benefits Ordinance

Contractor shall comply with all laws relating to the provision of benefits to its employees and their spouses or domestic partners, including, but not limited to, such laws prohibiting discrimination in the provision of such benefits on the basis that the spouse or domestic partner of the Contractor's employee is of the same or opposite sex as the employee.

e. Discrimination Against Individuals with Disabilities

The nondiscrimination requirements of 41 C.F.R. 60-741.5(a) are incorporated into this Agreement as if fully set forth here, and Contractor and any subcontractor shall abide by the requirements of 41 C.F.R. 60–741.5(a). This regulation prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified individuals with disabilities.

f. History of Discrimination

Contractor certifies that no finding of discrimination has been issued in the past 365 days against Contractor by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other investigative entity. If any finding(s) of discrimination have been issued against Contractor within the past 365 days by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or other investigative entity, Contractor shall provide County with a written explanation of the outcome(s) or remedy for the discrimination prior to execution of this Agreement. Failure to comply with this Section shall constitute a material breach of this Agreement and subjects the Agreement to immediate termination at the sole option of the County.

g. Reporting; Violation of Non-discrimination Provisions

Contractor shall report to the County Executive Officer the filing in any court or with any administrative agency of any complaint or allegation of discrimination on any of the bases prohibited by this Section of the Agreement or the Section titled "Compliance with Laws". Such

duty shall include reporting of the filing of any and all charges with the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other entity charged with the investigation or adjudication of allegations covered by this subsection within 30 days of such filing, provided that within such 30 days such entity has not notified Contractor that such charges are dismissed or otherwise unfounded. Such notification shall include a general description of the circumstances involved and a general description of the kind of discrimination alleged (for example, gender-, sexual orientation-, religion-, or race-based discrimination).

Violation of the non-discrimination provisions of this Agreement shall be considered a breach of this Agreement and subject the Contractor to penalties, to be determined by the County Executive Officer, including but not limited to the following:

i. termination of this Agreement;
ii. disqualification of the Contractor from being considered for or being awarded a County contract for a period of up to 3 years;
iii. liquidated damages of $2,500 per violation; and/or
iv. imposition of other appropriate contractual and civil remedies and sanctions, as determined by the County Executive Officer.

To effectuate the provisions of this Section, the County Executive Officer shall have the authority to offset all or any portion of the amount described in this Section against amounts due to Contractor under this Agreement or any other agreement between Contractor and County.

h. Compliance with Living Wage Ordinance

As required by Chapter 2.88 of the San Mateo County Ordinance Code, Contractor certifies all contractor(s) and subcontractor(s) obligated under this contract shall fully comply with the provisions of the County of San Mateo Living Wage Ordinance, including, but not limited to, paying all Covered Employees the current Living Wage and providing notice to all Covered Employees and Subcontractors as required under the Ordinance.

13. Compliance with County Employee Jury Service Ordinance

Contractor shall comply with Chapter 2.85 of the County's Ordinance Code, which states that Contractor shall have and adhere to a written policy providing that its employees, to the extent they are full-time employees and live in San Mateo County, shall receive from the Contractor, on an annual basis, no fewer than five days of regular pay for jury service in San Mateo County, with jury pay being provided only for each day of actual jury service. The policy may provide that such employees deposit any fees received for such jury service with Contractor or that the Contractor may deduct from an employee's regular pay the fees received for jury service in San Mateo County. By signing this Agreement, Contractor certifies that it has and adheres to a policy consistent with Chapter 2.85. For purposes of this Section, if Contractor has no employees in San Mateo County, it is sufficient for Contractor to provide the following written statement to County: "For purposes of San Mateo County's jury service ordinance, Contractor certifies that it has no full-time employees who live in San Mateo County. To the extent that it

hires any such employees during the term of its Agreement with San Mateo County, Contractor shall adopt a policy that complies with Chapter 2.85 of the County's Ordinance Code." The requirements of Chapter 2.85 do not apply unless this Agreement's total value listed in the Section titled "Payments", exceeds two-hundred thousand dollars ($200,000); Contractor acknowledges that Chapter 2.85's requirements will apply if this Agreement is amended such that its total value exceeds that threshold amount.

14. Retention of Records; Right to Monitor and Audit

(a) Contractor shall maintain all required records relating to services provided under this Agreement for three (3) years after County makes final payment and all other pending matters are closed, and Contractor shall be subject to the examination and/or audit by County, a Federal grantor agency, and the State of California.

(b) Contractor shall comply with all program and fiscal reporting requirements set forth by applicable Federal, State, and local agencies and as required by County.

(c) Contractor agrees upon reasonable notice to provide to County, to any Federal or State department having monitoring or review authority, to County's authorized representative, and/or to any of their respective audit agencies access to and the right to examine all records and documents necessary to determine compliance with relevant Federal, State, and local statutes, rules, and regulations, to determine compliance with this Agreement, and to evaluate the quality, appropriateness, and timeliness of services performed.

15. Merger Clause; Amendments

This Agreement, including the Exhibits and Attachments attached to this Agreement and incorporated by reference, constitutes the sole Agreement of the parties to this Agreement and correctly states the rights, duties, and obligations of each party as of this document's date. In the event that any term, condition, provision, requirement, or specification set forth in the body of this Agreement conflicts with or is inconsistent with any term, condition, provision, requirement, or specification in any Exhibit and/or Attachment to this Agreement, the provisions of the body of the Agreement shall prevail. Any prior agreement, promises, negotiations, or representations between the parties not expressly stated in this document are not binding. All subsequent modifications or amendments shall be in writing and signed by the parties.

16. Controlling Law; Venue

The validity of this Agreement and of its terms, the rights and duties of the parties under this Agreement, the interpretation of this Agreement, the performance of this Agreement, and any other dispute of any nature arising out of this Agreement shall be governed by the laws of the State of California without regard to its choice of law or conflict of law rules. Any dispute arising out of this Agreement shall be venued either in the San Mateo County Superior Court or in the United States District Court for the Northern District of California.

17. Notices

Any notice, request, demand, or other communication required or permitted under this Agreement shall be deemed to be properly given when both: (1) transmitted via facsimile to the telephone number listed below or transmitted via email to the email address listed below; and (2) sent to the physical address listed below by either being deposited in the United States mail, postage prepaid, or deposited for overnight delivery, charges prepaid, with an established overnight courier that provides a tracking number showing confirmation of receipt.

In the case of County, to:

Name/Title:	Michael Wentworth, ISD CIO
Address:	455 County Center, Fl 3
Telephone:	(650) 363-4710
Email:	mwentworth@smcgov.org

In the case of Contractor, to:

Name/Title:	Harish R. Rao, CEO, Interpersonal Frequency
Address:	P.O. Box 51, McLean VA 22101
Telephone:	(703) 400-6776
Email:	harish@ifsight.com

18. Electronic Signature

Both County and Contractor wish to permit this Agreement and future documents relating to this Agreement to be digitally signed in accordance with California law and County's Electronic Signature Administrative Memo. Any party to this Agreement may revoke such agreement to permit electronic signatures at any time in relation to all future documents by providing notice pursuant to this Agreement.

19. Payment of Permits/Licenses

Contractor bears responsibility to obtain any license, permit, or approval required from any agency for work/services to be performed under this Agreement at Contractor's own expense prior to commencement of said work/services. Failure to do so will result in forfeit of any right to compensation under this Agreement.

20. Reimbursable Travel Expenses

To the extent that this Agreement authorizes reimbursements to Contractor for travel, lodging, and other related expenses as defined in this section, the Contractor must comply with all the terms of this section in order to be reimbursed for travel.

a. Estimated travel expenses must be submitted to authorized County personnel for advanced written authorization before such expenses are incurred. Significant differences

between estimated and actual travel expenses may be grounds for denial of full reimbursement of actual travel expenses.

b. Itemized receipts (copies accepted) for all reimbursable travel expenses are required to be provided as supporting documentation with all invoices submitted to the County.

c. Unless otherwise specified in this section, the County will reimburse Contractor for reimbursable travel expenses for days when services were provided to the County. Contractor must substantiate in writing to the County the actual services rendered and the specific dates. The County will reimburse for travel at 75% of the maximum reimbursement amount for the actual costs of meals and incidental expenses on the day preceding and/or the day following days when services were provided to the County, provided that such reimbursement is reasonable, in light of travel time and other relevant factors, and is approved in writing by authorized County personnel.

d. Unless otherwise specified within the contract, reimbursable travel expenses shall not include Local Travel. "Local Travel" means travel entirely within a fifty-mile radius of the Contractor's office and travel entirely within a fifty-mile radius of San Mateo County. Any mileage reimbursements for a Contractor's use of a personal car for reimbursable travel shall be reimbursed based on the Federal mileage reimbursement rate.

e. The maximum reimbursement amount for the actual lodging, meal and incidental expenses is limited to the then-current Continental United States ("CONUS") rate for the location of the work being done (i.e., Redwood City for work done in Redwood City, San Mateo for work done at San Mateo Medical Center) as set forth in the Code of Federal Regulations and as listed by the website of the U.S. General Services Administration (available online at http://www.gsa.gov/portal/content/104877 or by searching www.gsa.gov for the term 'CONUS'). County policy limits the reimbursement of lodging in designated high cost of living metropolitan areas to a maximum of double the then-current CONUS rate; for work being done outside of a designated high cost of living metropolitan area, the maximum reimbursement amount for lodging is the then-current CONUS rate.

f. The maximum reimbursement amount for the actual cost of airfare shall be limited to fares for Economy Class or below. Air travel fares will not be reimbursed for first class, business class, "economy-plus," or other such classes. Reimbursable car rental rates are restricted to the mid-level size range or below (i.e. standard size, intermediate, compact, or subcompact); costs for specialty, luxury, premium, SUV, or similar category vehicles are not reimbursable. Reimbursable ride-shares are restricted to standard or basic size vehicles (i.e., non-premium vehicles unless it results in a cost-saving to the County). Exceptions may be allowed under certain circumstances, such as unavailability of the foregoing options, with written approval from authorized County personnel. Other related travel expenses such as taxi fares, ride-shares, parking costs, train or subway costs, etc. shall be reimbursable on an actual-cost basis. Reimbursement of tips for taxi fare, or ride-share are limited to no more than 15% of the fare amount.

g. Travel-related expenses are limited to: airfare, lodging, car rental, taxi/ride-share plus tips, tolls, incidentals (e.g. porters, baggage carriers or hotel staff), breakfast, lunch, dinner, mileage reimbursement based on Federal reimbursement rate. The County will not reimburse for alcohol.

h. Reimbursement of tips are limited to no more than 15 percent. Non-reimbursement items (i.e., alcohol) shall be excluded when calculating the amount of the tip that is reimbursable.

21. Prevailing Wage

When applicable, Contractor hereby agrees to pay not less than prevailing rates of wages and be responsible for compliance with all the provisions of the California Labor Code, Article 2-Wages, Chapter 1, Part 7, Division 2, Section 1770 et seq. A copy of the prevailing wage scale established by the Department of Industrial Relations is on file in the office of the Director of Public Works, and available at www.dir.ca.gov/DLSR or by phone at 415-703-4774. California Labor Code Section 1776(a) requires each contractor and subcontractor keep accurate payroll records of trades workers on all public works projects and to submit copies of certified payroll records upon request.

Additionally,
• No contractor or subcontractor may be listed on a bid proposal for a public works project (submitted after March 1, 2015) unless registered with the Department of Industrial Relations pursuant to Labor Code section 1725.5 [with limited exceptions from this requirement for bid purposes only under Labor Code section 1771.1(a)].

• No contractor or subcontractor may be awarded a contract for public work on a public works project (awarded on or after April 1, 2015) unless registered with the Department of Industrial Relations pursuant to Labor Code section 1725.5.

• This project is subject to compliance monitoring and enforcement by the Department of Industrial Relations

22. Limitations of Liability

In no event will either Party be liable under or in connection with this Agreement under any legal or equitable theory, for any: (a) consequential, incidental, indirect, exemplary, special, enhanced, or punitive damages; (b) increased costs, diminution in value or lost business, production, revenues, or profits; (c) use, inability to use, interruption, delay or recovery of any data. In no event will either Party's aggregate liability arising out of or related to this Agreement under any legal or equitable theory exceed the total amounts paid to Contractor by County under this Agreement during the twelve (12) month period preceding the event giving rise to such claim(s).

* * *

In witness of and in agreement with this Agreement's terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: INTERPERSONAL FREQUENCY, LLC

Contractor Signature	Date	Contractor Name (please print)
	10/11/2022	Harish Rao

COUNTY OF SAN MATEO

By:

President, Board of Supervisors, San Mateo County

Date:

ATTEST:

By:

Clerk of Said Board

Exhibit A

In consideration of the payments set forth in Exhibit B, Contractor shall provide the following services:

Definitions

DNS - Domain Name System: Manages the mapping between names and numbers. DNS servers translate requests for names into IP addresses.

PHP - Hypertext Preprocessor: Scripting language.

SSO - Single Sign On: Authentication scheme that allows users to log in with a single ID to any of several related, yet independent, software systems.

CDN - Content Delivery Network: Refers to a geographically distributed group of servers that work together to provide fast delivery of internet content.

CMS - Content Management System: Software that helps create, manage, and modify content on a website. (i.e. Drupal).

SAML - Security Assertion Markup Language: Enables access to multiple web applications using one set of login credentials.

WAF - Web Application Firewall: Helps protect web applications against common web exploits and bots.

HTTPS - Hypertext Transfer Protocol Secure: Used for secure communication over a computer network.

Migration Plan

Migrate Drupal-level redirects and transition from Acquia SOLR to Elastic Site Search.

Drupal-level Redirects

1. County sends the list of redirects.
2. Contractor configures the page level redirects in Drupal using the bulk redirects module.
3. Contractor will configure the server level redirects in partnership with County using a combination of County's DNS and our platform tools. Note, because of the number of server level redirects, we cannot guarantee that all will be configured by launch. We will coordinate this process and timing with the County team.
4. Test and validate.

Elastic Site Search Migration Plan

1. Contractor evaluates the County's site (content types, types of files currently being indexed, etc.) This would also require looking at the custom fields that are being indexed.
2. Contractor works with County team to determine items like:
    a. Setting priority levels for data points (what shows up higher in results)
    b. SOLR specifics such as autocomplete and fuzzy search
3. Contractor creates a County account using Elastic Site Search.
4. Contractor creates the configuration.
5. Contractor completes the migration, including testing.
6. County team gains access to the administration portal.

7. Contractor trains County team on the administration portal.

Task Based Migration Plan with Tentative Dates

Once Contractor gains access to the database Contractor can review and update the plan and timeline above.

TASK	Tentative Dates
1. Contractor gains access to the County database and reviews to confirm understanding.	10/24/2022
2. Contractor works with County to discuss any questions related to the code base and database.	10/21/2022 –10/28/2022
3. Contractor creates environments in Fulcrum.	10/24/2022
4. Contractor begins the process of configuring the site from Acquia to Fulcrum standards.	10/25/2022
5. Contractor begins the process to transition SOLR to ElasticSiteSearch.	10/31/2022
6. Contractor begins transition of codebase to Bitbucket.	10/31/2022
7. Contractor schedules cutover date with County, along with scheduled code and content freezes.	11/14/2022
8. Cutover is completed.	11/28/2022

Support & Maintenance

Contractor will support and maintain the full Drupal application stack and all customizations, including:

- Drupal application (smcgov.org)
- MySQL database
- PHP
- All Drupal modules, customizations, and enhancements
- Custom-built REACT-based content editor (https://react-page.github.io/)
- Outline design system (https://github.com/phase2/outline/)
- Unlimited URL and page level redirects to Drupal resources
    - Redirection from Subdomain to a specific Drupal node, e.g. food.smcgov.org > https://www.smcgov.org/food
    - Redirection from vanity domain to a specific Drupal node, e.g. smcpdu.org > https://www.smcgov.org/cmo/pdu

    - Redirection from legacy Drupal 7 nodes to Drupal 9 nodes, e.g. bos.smcgov.org/1999-board-agendas > https://www.smcgov.org/bos/1999-board-agendas
    - Catch-all redirects from legacy Drupal 7 nodes to department landing pages for any legacy subdomain URI redirection to Drupal 9 landing page. E.g. bos.smcgov.org/xyz to https://www.smcgov.org/bos.
- SSO integration for all Drupal environments with County's SSO provider
- Website search functionality and integration with search service
- Hosting environment and web server configuration
- Website security, infrastructure and CDN
- Website design and development
- Drupal CMS development
- System administration
- Maintenance and support of installed modules and custom enhancements
- Cloud hosting for the County's Drupal website, CMS and all the supporting features and functionality required by the system as configured

Evolution & Support Plan	Provides expanded Drupal support and digital strategy to grow online impact and viewership. Suitable for organizations that have some internal web developer staff but wish to augment internal resources. ● Includes up to 80 hours of consulting & support monthly, with unused hours expiring monthly. ● Support is available via our toll-free phone number or support portals for any request. ● Additional time may be "borrowed" from future months (with the expectation that planned work will be coordinated in advance). ● Project Manager available if needed.
Fulcrum Cloud Hosting	● 99.9% uptime guarantee. ● Includes 800,000 pageviews per month, 400GB database and file storage, and up to 1TB of data transfer per month (not metered) — no additional charges assuming this average is not exceeded on a rolling 180-day basis. ● Includes hosting maintenance. This does not include changes to the CMS platform itself other than security updates and patches. Additional developer support is covered by Evolution & Support plans (see options below). ● Includes URL redirection service and SOLR hosting for San Mateo County ● Includes Voice of Citizen® Subscription with Semi-Annual Reporting. ● See Exhibit C for additional terms and conditions. The terms and conditions of this agreement will take precedence over

	contradictory terms and conditions as listed in Exhibit C. ● Note: This fee must be paid yearly.
Advanced Authentication	Integration with an existing Identity and Access Management (IAM) service, via SAML. Assumes Okta as the identity provider. This option is subject to further technical scoping. Initial onboarding and any future maintenance are to be deducted from Evolution & Support plan hours.
CitizenSecure Hosting Bundle	● Extended Backup Retention Fulcrum includes retention of backups from production and other environments on a rolling 7-day basis, with the oldest backups automatically deleted. This option extends retention: the one (1) weekly backup is preserved each week for 6 months, on a rolling basis. ● WAF / CDN /DDos Protection Increased uptime guarantee to 99.95% ● Large File Uploads Fulcrum includes uploading and managing files 14MB or less through the Drupal core and media module. This option is for the ability to upload large files (greater than 14MB and up to 5GB). ● Bulk File Uploads Adds the ability to support multiple uploads at a time.
Elastic Site Search	Contractor Provided Elastic Site Search upgrade from Solr. Includes crawling domains that are part of the smcgov.org domain (e.g., Drupal 9 site content like smcgov.org/da or parks.smcgov.org). County team will have full admin control and direct access to the administrative interface.
Elastic Site Search - non-SMCgov.org domains	Add $500 per year for each non-SMCgov.org website (e.g., smchealth.org or smcl.org). At time of contracting, there are a total of 6 websites. If additional sites are needed to be crawled, a $500 / year per site fee will be charged.
Onboarding	This is required to transition from Acquia to Fulcrum cloud hosting and is based on an

	assumption of 50 hours to complete the transition. It is waived should the County elect a multi-year contract with a Sustain or higher-level Evolution & Support plan.

Additional Projects

Contractor can provide enhancements to the current website outside of the Evolution and Support plan. Such projects will be initiated by the County's Information Services Department (ISD) and task order generated. Projects to be individually scoped and mutually agreed upon. Other departments, with approval from the County's ISD and Contractor, can enter into a separate agreement with Contractor for department-specific enhancements and services as listed below. These agreements will be executed on a mutually agreed upon template provided by ISD.

Such projects include department-specific enhancements such as the following:

- Drupal CMS development, customizations, and enhancements
- Drupal modules, customizations, and enhancements
- Custom-built REACT-based content editor customizations and enhancements
- Outline design system customizations and enhancements
- Website design and development services
- Website Search functionality and search service integration
- Hosting environment and web server configuration

Exhibit B

In consideration of the services provided by Contractor described in Exhibit A and subject to the terms of the Agreement, County shall pay Contractor based on the following fee schedule and terms:

Pricing Totals for 3 Years

Item	Year 1 Cost	Year 2 Cost	Year 3 Cost
Evolution & Support Plan	$ 153,600.00	$ 161,280.00	$ 169,344.00
Fulcrum Cloud Hosting	$ 33,716.00	$ 35,401.80	$ 37,171.89
CitizenSecure Hosting Bundle	$ 7,840.00	$ 8,232.00	$ 8,643.60
Elastic Site Search	$ 7,750.00	$ 8,137.50	$ 8,544.38
Elastic Site Search - non-SMCgov.org domains	$ 3,000.00	$ 3,150.00	$ 3,307.50
TOTAL:	$ 205,906.00	$ 216,201.30	$ 227,011.37
		NOT TO EXCEED AMOUNT:	$ 649,118.67

Pricing Assumptions

- County will provision high-availability, preferably via an external cloud-based, DNS provider and for supporting DNS updates and changes. Failure to provide highly available DNS may invalidate SLA uptime commitments.
- The project schedule, timeline and fees are predicated on prompt County responses, active participation in the project, adequate County staff resource commitments, and requested data delivery in a timely manner from County. Excessive delays will cause schedule and cost increases. If County requests or causes time delays that extend the project beyond the agreed-upon time frames a change order will be necessary.
- HTTPS must be enforced throughout the website and related County applications. The County is responsible for ensuring this with other web applications.
- Pricing above assumes use of our Fulcrum Premier hosting and Contractor's evolution and support plan. See Exhibit C for additional terms and conditions. The terms and conditions of this agreement will take precedence over contradictory terms and conditions as listed in Exhibit C.
- County has the perpetual, non-expiring license to use the software and all improvements made as a result of this agreement, as well as to modify and share it with others as you see fit. However, since Drupal is open source, updates made to the core platform as part of this project will be contributed to the Drupal community to benefit other Drupal users.

Additional Projects

In consideration of the services for additional projects provided by Contractor are based on the following fee schedule and terms.

Role	Cost
Staff Hourly Rate	$175.00 / hour
DevOps Staff Hourly Rate	$400.00 / hour
Content-Related Services	$155.00 / hour

Invoicing

County shall pay Contractor, upon receipt of an invoice, for services rendered. Each invoice submitted must include the following, at a minimum:

Payments shall be made within Net 30 days from the date of the applicable, undisputed invoice.

- Agreement Number or PO Number
- Time period covered
- Detailed statement of services/work completed for the invoice period
- Breakdown of labor, materials, and taxes if applicable
- A detailed breakdown of hours used by function. For example:
    - Development hours used
    - Project management hours used
    - DevOps hours used
- An itemized list of tickets started, worked and/or completed each month.

Fulcrum, Voice of Citizen®, Voice of Patron®: I.F. SaaS Services Agreement: Spring 2021 Version

Exhibit C: Software-as-a-Service Agreement 3
- RECITALS 3
- AGREEMENT 3
- Definitions. 3
- Access and Use. 4
- Service Levels & Support; Cloud Provider Terms. 6
- Client Responsibilities. 7
- Data Protection Terms. 7
- Limited Warranty and Warranty Disclaimer. 9
- Limitations of Liability. 9
- Miscellaneous. 9

EXHIBIT A: STATEMENT OF WORK 13

EXHIBIT D: PREMIER SERVICE LEVEL AGREEMENT; SUPPORT & MAINTENANCE TERMS 14
- Fulcrum Cloud Services: Managed Hosting with Drupal CMS Care 14
- Standard Maintenance 14
- Scheduled Maintenance: Covered by Separate I.F. Support Plan 20
- Emergency Maintenance 20
- Hours of Operation 21
- Getting Support for Fulcrum SaaS or for I.F. Support Plans 21
- Uptime Commitment and Exclusions 21
- Emergency Service Conditions 22
- Response Time Goals 23
- Service Credit 24
- Infrastructure, Scaling, and Redundancy 24
- Database and File size 24
- Page Views & Bandwidth 24
- Backups 25
- Infrastructure 25
- Voice of Patron®/Voice of Citizen® SaaS analytics service 25
- Drupal Support from our Solutions Engineering Team 25
- Disaster Recovery 25
- Network Outage Scenario 26
- Severe Cloud Server or Infrastructure Failure Scenario 26
- Data Center Disaster Scenario 26

Security for Fulcrum Cloud Services & SaaS Services 26
Security Monitoring & Network Intrusion Protection 27
Denial of Service Protection 27
Data Center Security 28
I.F. Employee Administrative Access 28
Releasing Patches and Updates 28

Interpersonal Frequency Privacy Policy Effective: 9/1/2018 30
Information We Collect 30
Personally-Identifying Information 30
Information Collected for Others 31
Cookies 31
How We Share the Information We Collect With Others 31
How to Access Your Information 32
Security Measures We Take to Protect Your Information 32
Privacy Policy Is Subject to change 32

Exhibit E: Terms of Service for Voice of Citizen® and/or Voice of Patron® SaaS 33
Voice of Citizen® / Voice of Patron® Service 33
Acceptable Use Policies 33
Enforcement 34
Unauthorized Activities 34
Your Representations 34
Termination of Services for Voice of Citizen® and/or Voice of Patron® SaaS 34
Refund Policy for Voice of Citizen® and/or Voice of Patron® SaaS 35
Information and Intellectual Property Rights for Voice of Citizen® and/or Voice of Patron® SaaS 35

Exhibit C: Software-as-a-Service Agreement

THIS INTERPERSONAL FREQUENCY LLC SOFTWARE AS A SERVICE AGREEMENT (this "Agreement"), by and between INTERPERSONAL FREQUENCY LLC (I.F.) and the Client identified in the MSA or SOW (as defined below) is executed by and between such entities as of the effective date of such SOW or MSA ("Effective Date") for the products and services described herein and therein;

RECITALS

WHEREAS, the Parties have negotiated the terms of an I.F. Master Services Agreement, other named I.F. services agreement or a Client form of services agreement (collectively, the "MSA") by which I.F. will perform and provide certain products or professional services to Client (collectively, "Professional Services"); and

WHEREAS, in connection with the performance and delivery of the Professional Services and any and all other materials and work product covered by the MSA and/or this Agreement (collectively "Deliverables"), the Client desires to have access to I.F's Software platform tools and functions (the "Software as a Service" or the "SaaS Services") and any other products or services set forth in any exhibit hereto on the terms and conditions hereof and thereof.

AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties do hereby agree as follows:

1. Definitions.

As used in this Agreement, the following capitalized terms shall mean and be interpreted as follows:

(a) "Aggregated Statistics" means data and information related to Client's use of the Software and the SaaS Services (but which do not personally identify or profile Client or its Authorized Users) that are collected or received by I.F. in an aggregated and anonymized manner, including to compile statistical and performance information relating to the SaaS Services and data regarding Client's and its Authorized Users' use of the SaaS Services and the web site on which the SaaS Serves are hosted or by which I.F.'s services are accessed or delivered.

(b) "Authorized User" means Client's employees, consultants, contractors, agents, web site visitors or other permitted users who or which are authorized by Client to access and use the SaaS Services under the rights granted to Client hereunder.

(c) "Client Data" means, other than Aggregated Statistics, information, data and other content, in any form or medium, that is submitted, posted, transmitted or otherwise provided by or on behalf of Client or an Authorized User in the Software or through the SaaS Services.

(d) "Documentation" means I.F.'s user manuals, handbooks and guides relating to the SaaS Services provided to Client hereunder, either electronically or in hard copy form, and any and all other Client or end user documentation relating to the SaaS Services.

(e) "Cloud Provider" means the provider of Cloud Services which, as of the Effective Date hereof, is Amazon Web Services ("AWS"), but such term includes any and all successors or additional hosting providers thereto.

(f) "Cloud Services" means the provision of on-demand online access to the SaaS Services and all hardware, software, computing power and resources relating thereto.

(g) "I.F. Intellectual Property" or "I.F. IP" means the SaaS Services, the Documentation and any and all other intellectual property provided to Client or any Authorized User in connection with the foregoing. For the avoidance of doubt, I.F. IP includes Aggregated Statistics and any and all other information, data or other content derived from I.F.'s monitoring of Client's or an Authorized User's access to or use of the SaaS Services, but does not include Client Data.

(h) "Service Level Agreement" or "SLA" means the agreement attached as Exhibit D, and all amendments or revisions thereto which shall automatically be incorporated into and made a part of this Agreement.

(i) "Statement of Work" or "SOW" means the document attached as Exhibit A, which may take the form of a "Quote & Order Form for Services or Software Subscription" (or other form), and all amendments or revisions thereto which shall automatically be incorporated into and made a part of this Agreement.

(j) "Software" the source code and object code and any and all other software tools, functionalities and information necessary to use, operate and maintain the SaaS Services.

(k) "SaaS Services" means the software-as-a-service offering described in Exhibits A and D and includes, if selected and paid for by Client, access to and use of I.F.'s proprietary software data analytics tools or products known as "Fulcrum" and/or "Voice of Patron®," and/or "Voice of Citizen®," as modified from time to time, and any other I.F. tools, functions or capabilities.

(l) "Third-Party Products" means any third-party products described in Exhibit A or Exhibit D provided with or incorporated into the Software or SaaS Services.

2. Access and Use.

(a) Provision of Access. Subject to and conditioned upon Client's payment of all Fees associated with the Deliverables provided to Client under the MSA, this Agreement and any other agreement or understanding between the Parties, and compliance with all other terms and conditions hereof and thereof, I.F. hereby grants to Client a non-exclusive, non-transferable (except in compliance with Section 12(g)) right to access and use the SaaS Services during the Term, solely for use by Authorized Users in accordance with the terms and conditions hereof. Such use is limited to Client's internal business use and operations. I.F. shall provide to Client

the necessary passwords and network links or connections to allow Client to access the SaaS Services. The number of Authorized Users is not expressly limited unless so indicated in the SOW, but concurrent use of the SaaS Services shall be subject to the technical capabilities of the I.F. infrastructure and the devices and connectivity of the Authorized Users.

(b) Documentation License. Subject to the terms and conditions contained in this Agreement, I.F. hereby grants to Client a non-exclusive, non-transferable (except in compliance with Section 12(g)) license to use the Documentation during the Term solely for Client's internal business purposes in connection with its use of the SaaS Services.

(c) Use Restrictions. Client shall not use the SaaS Services or the Documentation, in whole or in part, including any integrated I.F. products or Third Party Products, for any purposes beyond the scope of the rights of access granted in this Agreement. Client shall not at any time, directly or indirectly, and shall not permit any Authorized Users to: (i) copy, modify, or create derivative works of the SaaS Services, the Software or the Documentation, in whole or in part; (ii) rent, lease, lend, sell, license, sublicense, assign, distribute, publish, transfer, or otherwise make available the SaaS Services or the Documentation; (iii) reverse engineer, disassemble, decompile, decode, adapt or otherwise attempt to derive or gain access to the Software or any other element of the SaaS Services, in whole or in part; (iv) remove any proprietary notices from the SaaS Services or Documentation; or (v) use the SaaS Services or Documentation in any manner or for any purpose that infringes, misappropriates or otherwise violates any intellectual property right or other right of any person or that violates any applicable law or regulation.

(d) Reservation of Rights. I.F. reserves all rights and interests not expressly granted to Client in this Agreement. Except for the limited rights and licenses expressly granted under this Agreement, nothing in this Agreement grants, by implication, waiver, estoppel or otherwise, to Client, to any Authorized Users or to any third party any intellectual property rights or other right, title or interest in or to the I.F. IP, the Software, the Documentation or the SaaS Services.

(e) Suspension or Termination of SaaS Services. Notwithstanding anything to the contrary in this Agreement, I.F. may, at its option, temporarily suspend Client's and/or any Authorized User's access to any portion or all of the SaaS Services, without termination of this Agreement, or terminate this Agreement and all of Client's and its Authorized User's access to SaaS Services in the event that:

(i) I.F. reasonably determines that (A) there is a threat or attack on any of the I.F. IP or any Cloud Provider's I.P.; (B) Client's or any Authorized User's use of the I.F. IP disrupts or poses a security risk to the I.F. IP, to Cloud Provider's I.P. or to any other customer or vendor of I.F.; (C) Client or any Authorized User is using the I.F. IP for fraudulent or illegal activities or in violation of I.F.'s or the Cloud Provider's acceptable use policy or any other policies; (D) subject to applicable law, Client has ceased to continue its business in the ordinary course, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding; or (E) I.F.'s provision of the SaaS Services to Client or to any Authorized User is prohibited by applicable law;

(ii) any vendor of I.F., including but not limited to, the Cloud Provider, has suspended or terminated I.F.'s access to or use of any third-party services or products required to enable Client to access the Services; or

(iii) in accordance with Section 5(a)(iii) (any such suspension or termination described in sub-paragraph (i), (ii), or (iii) above, a "Services Suspension" or a "Services Termination" as applicable).

(iv) I.F. shall use commercially reasonable efforts to provide written notice of any Services Suspension or Services Termination to Client and to provide updates regarding resumption of access to the Services following any Service Suspension. I.F. shall use commercially reasonable efforts to resume providing access to the SaaS Services as soon as reasonably practicable after the event giving rise to a Services Suspension is cured. I.F. WILL HAVE NO LIABILITY FOR ANY DAMAGES, LIABILITIES, LOSSES (INCLUDING ANY LOSS OF DATA OR PROFITS), OR ANY OTHER CONSEQUENCES THAT CLIENT OR ANY AUTHORIZED USER MAY INCUR AS A RESULT OF A SERVICES SUSPENSION OR SERVICES TERMINATION.

(f) Aggregated Statistics. Notwithstanding anything to the contrary in this Agreement, I.F. may electronically log and monitor Client's and any and all Authorized User's use of the SaaS Services and collect and compile Aggregated Statistics. As between I.F. and Client, all right, title, and interest in Aggregated Statistics, and all intellectual property rights therein, belong to and are granted and retained solely by I.F. and such rights are hereby waived and released by Client. Client acknowledges that I.F. may compile Aggregated Statistics based on Client Data input into the SaaS Services. Client agrees that I.F. may (i) make Aggregated Statistics publicly available in compliance with applicable law, and (ii) use Aggregated Statistics to the extent and in the manner permitted under applicable law; provided that the publication, release or transfer of such Aggregated Statistics do not identify personally Client or its Authorized users or disclose Client's Confidential Information.

(g) Cloud Services. I.F. has contracted with the Cloud Provider to make Cloud Services available to Client and any and all Authorized Users. Any SaaS Services-related issues that are caused or contributed to by outages or other problems with the Cloud Services should be promptly referred to I.F. for handling. Client acknowledges and agrees on its own behalf and on behalf of all Authorized Users that the Cloud Services are provided by the Cloud Provider and the Cloud Provider, which retains the unlimited right to service, make modifications and/or enhancements to and manage the Cloud Services at any time in its discretion. Client and Authorized Users shall at all times have online access to the applicable terms of service, service level agreements and acceptable use policies of the Cloud Provider which are hereby integrated into and made a part of this Agreement in Section 3 below. Execution of this Agreement constitutes Client's approval of such terms and conditions, on its own behalf and on behalf of all Authorized Users.

3. Service Levels & Support; Cloud Provider Terms.

(a) Modifications to SaaS Services or Software. Client hereby acknowledges and agrees that I.F. may, at any time without prior notice, change, modify, enhance or alter any features, functions or capabilities of the SaaS Services or the Software, in its sole discretion,

without affecting any term or condition of this Agreement (including Fees) so long as such changes do not materially and adversely affect Client's overall user experience or efficiency.

(b) Service Levels. Subject to the terms and conditions of this Agreement, I.F. shall use commercially reasonable efforts to make the SaaS Services available in accordance with the service levels set out in the attached Exhibit D, which is hereby incorporated herein.

(c) Support. The access rights granted hereunder entitles Client to the SaaS support services described on Exhibit D for ongoing and continuous one-year periods following the Effective Date hereof, if and to the extent that Client purchases such support services at the Fees applicable thereto.

(d) Client Data Recovery & Retention. During the Term hereof, Client shall have the right to access, download and use all Client Data, included all Authorized User data, in its discretion and as permitted by applicable law, the obligations of which shall be Client's sole responsibility. Notwithstanding the foregoing, Client must recover any and all Client Data that it desires to receive and retain not later than ninety (90) days after termination of this Agreement, regardless of cause (the "Data Recovery Period"). After expiration of the Data Recovery Period, I.F. may destroy or delete all Client Data from all I.F. computers, services and cloud instances.

4. Client Responsibilities.

(a) General. Without prejudice to any and all duties and obligations of Client hereunder under any other agreement, Client is responsible and liable for all uses of the SaaS Services and Documentation resulting from any access provided or permitted by Client, directly or indirectly, whether such access or use is permitted by or in violation of this Agreement. Without limiting the generality of the foregoing, Client is responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User that would constitute a breach of this Agreement if taken by Client will be deemed a breach of this Agreement by Client. Client shall make all Authorized Users aware of their duties and obligations hereunder as applicable to their respective use of the SaaS Services and shall cause Authorized Users to comply with all such requirements.

(b) Third-Party Products. I.F. may from time to time, upon request by Client or otherwise, make Third-Party Products available to Customer independently of the SaaS Services by separate agreement or as an element hereof. For purposes of this Agreement, such Third-Party Products are subject to their own terms and conditions (wherever memorialized) and, only if hosted or supported by I.F., will be subject to any applicable flow through provisions referred to in Exhibit A or Exhibit D as applicable. If Client does not agree to abide by the applicable terms for any such Third-Party Products, then Client should not install or use such Third-Party Products.

5. Data Protection Terms.

For purposes of this Section 8, the following terms shall mean as follows:

"*Business*" means as defined in the CCPA.

"*CCPA*" means the California Consumer Privacy Act, Cal. Civ. Code §1798.100 et. seq.

"*Data Protection Laws*" means all applicable laws, regulations and requirements in any jurisdiction relating to data privacy, data protection, data security and/or the processing of Personal Information, including, without limitation, the CCPA.

"*Data Subject*" means an identified or identifiable natural person about whom Personal Information relates, including a "consumer" as defined in the CCPA.

"*Data Subject Rights*" means those rights identified in the CCPA as granted to Data Subjects.

"*Personal Information*" includes any personally identifiable information as defined by applicable Data Protection Laws and includes any Client Data which meets such definition.

"*Process*" and "*Processing*" means any one or more operations performed on personal information, whether or not by automated means.

"*Sale*" or "*sell*" means as defined in the CCPA.

"*Security Breach*" means (i) the loss or misuse of Client Data; or (ii) the inadvertent, unauthorized and/or unlawful Processing, disclosure, access, alteration, corruption, transfer, sale, rental, destruction or use of any Client Data.

"*Service Provider*" means as defined in the CCPA.

(a) Client hereby represents, warrants and covenants to I.F. that Client has provided or will provide timely, correct and complete privacy notices to all Data Subjects included in Client Data in compliance with all applicable Data Protection Laws. Client further represents, warrants and covenants to I.F. that Client has obtained or will obtain timely, transparent, informed, voluntary and complete consents from all Authorized Users as required by Data Protection Laws for Client's use of the SaaS Services and Software, including (i) consent to I.F.'s collection, use, and disclosure of Client Data (to the extent such data includes Personal Information) and (ii) I.F.'s Processing, use, storage and transfer of Client Data relating to Client's and Authorized Users' use of the SaaS Services and Software.

(b) For CCPA purposes, if and as applicable, the parties agree that I.F. is or shall be deemed to be a Service Provider to the Client for all purposes covered by this Agreement. Accordingly, the parties hereby agree that I.F.'s access to and use of any and all Client Data uploaded into the SaaS Services and/or Software or otherwise provided to or made available to I.F. which constitutes Personal Information is subject to the following agreements and restrictions:

(i) The Client is providing such Client Data only as necessary for I.F. to carry out the business purposes represented by this Agreement;

(ii) I.F. agrees not to retain, use or disclose the Client Data for any purpose except to perform this Agreement for the Client;

(iii) I.F. agrees not to sell, disclose or provide access to the Client Data to any third party except to the Cloud Provider and then solely to

perform the Cloud Services for the benefit of the Client. Client's execution of this Agreement constitutes Client's consent to all such uses and disclosure by I.F. to the Cloud Provider; and

(iv) I.F. agrees to cooperate with and support the Client's compliance with and response to any consumer's exercise of its Data Subject Rights under the CCPA relating to any Client Data held by I.F. or by the Cloud Provider; *provided that* I.F.'s sole obligation to the Cloud Provider is to notify it of any such exercise of Data Subject Rights and carry out Client's instructions with regard thereto.

(c) I.F. agrees to take all reasonable actions to Process any Personal Information subject to Data Protection Laws only in accordance with Client's instructions solely to perform the terms and conditions of this Agreement for the sole benefit of the Client.

(d) If either party believes that a Security Breach has occurred, such party must notify the other party as promptly as possible without unreasonable delay. Each party will reasonably assist the other party in complying with and mitigating any potential damage resulting from a Security Breach in accordance with applicable Data Protection Laws.

6. Limited Warranty and Warranty Disclaimer.

I.F. warrants that the SaaS Services will conform in all material respects to the service levels set forth in this document when accessed and used in accordance with the Documentation and this Agreement. I.F. does not make any representations or guarantees regarding uptime or availability of the SaaS Services unless and to the limited extent specifically identified in this document. The remedies set forth in Exhibit D are Client's sole remedies and I.F.'s sole liability under the limited warranty set forth in this Section 8(a). THE FOREGOING WARRANTY DOES NOT APPLY TO, AND INTERPERSONAL FREQUENCY STRICTLY DISCLAIMS, ANY AND ALL WARRANTIES WITH RESPECT TO ANY CLOUD PROVIDER PRODUCTS OR SERVICES AND/OR THIRD-PARTY PRODUCTS.

EXCEPT FOR THE LIMITED WARRANTY SET FORTH IN SECTION 8(a), THE INTERPERSONAL FREQUENCY IP IS PROVIDED "AS IS" AND INTERPERSONAL FREQUENCY HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. INTERPERSONAL FREQUENCY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. EXCEPT FOR THE LIMITED WARRANTY SET FORTH IN SECTION 8(a), INTERPERSONAL FREQUENCY MAKES NO WARRANTY OF ANY KIND THAT THE INTERPERSONAL FREQUENCY IP, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CLIENT'S OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE.

7. Miscellaneous.

(a) Entire Agreement. This Agreement, together with the MSA and any and all other Exhibits and documents incorporated herein by reference, constitute the sole and integrated agreement of the Parties with respect to the subject matter hereof and supersedes all prior and

contemporaneous understandings, agreements, and representations and warranties, both written and oral, with respect to such subject matter. In the event of any conflict or inconsistency between the terms of this Agreement, the MSA, the related Exhibits, and any other documents incorporated herein by reference, the following order of precedence shall govern such conflict or inconsistency: (i) first, the MSA; (ii) second, this Agreement, excluding its Exhibits; (iii) third, the Exhibits to this Agreement (unless and to the extent they expressly override any provisions of the MSA or this Agreement); and (iv) fourth, any other documents incorporated herein by reference (unless and to the extent they expressly override any provisions of the MSA or this Agreement).

(b) Notices. All notices, requests, consents, claims, demands, waivers and other communications hereunder (each, a "Notice") must be in writing and addressed to the Parties at the addresses set forth on the first page of this Agreement (or to such other address that may be designated by the Party giving Notice from time to time in accordance with this Section). All Notices must be delivered by personal delivery, nationally recognized overnight courier (with all fees prepaid), facsimile or by email (with confirmation of transmission) or certified or registered mail (in each case, return receipt requested, postage prepaid). Except as otherwise provided in this Agreement, a Notice is effective only: (i) upon receipt by the receiving Party; and (ii) if the Party giving the Notice has complied with the requirements of this Section.

(c) Force Majeure. In no event shall I.F. be liable to Client or any Authorized User, or be deemed to have breached this Agreement, for any failure or delay in performing its obligations under this Agreement (except for any obligations to make payments), if and to the extent such failure or delay is caused by any circumstances beyond I.F.'s or any Cloud Provider's reasonable control, including but not limited to acts of God, flood, fire, earthquake, explosion, war, terrorism, invasion, riot or other civil unrest, strikes, labor stoppages or slowdowns or other industrial disturbances, or passage of law or any action taken by a governmental or public authority, including imposing an embargo.

(d) Amendment and Modification; Waiver. No amendment to or modification of this Agreement is effective unless it is in writing and signed by an authorized representative of each Party. No waiver by any Party of any of the provisions hereof will be effective unless explicitly set forth in writing and signed by the Party so waiving. Except as otherwise set forth in this Agreement, (i) no failure to exercise, or delay in exercising, any rights, remedy, power or privilege arising from this Agreement will operate or be construed as a waiver thereof, and (ii) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege.

(e) Severability. If any provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability will not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties shall negotiate in good faith to modify this Agreement so as to effectuate their original intent as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

(f) Assignment. Client may not assign any of its rights or delegate any of its obligations hereunder, whether voluntarily, involuntarily, by operation of law or otherwise, without the prior written consent of I.F. Any purported assignment or delegation in violation of

this Section will be null and void. No permitted assignment or delegation will relieve the assigning or delegating Party of any of its obligations hereunder. This Agreement is binding upon and inures to the benefit of the Parties and to the benefit of their respective permitted successors and assigns.

(g) Export Regulation. The SaaS Services utilize software and technology that may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations. Client shall not, directly or indirectly, export, re-export or release the SaaS Services or the underlying software or technology to, or make the SaaS Services or the underlying software or technology accessible from, any jurisdiction or country to which export, re-export or release is prohibited by law, policy, rule or regulation. Client shall comply with all applicable federal laws, regulations, and rules, and complete all required undertakings (including obtaining any necessary export license or other governmental approval), prior to exporting, re-exporting, releasing, or otherwise making the SaaS Services or the underlying Software or technology available outside the U.S.

(h) U.S. Government Rights. The Software and Documentation tools, components or functionalities comprising the SaaS Services constitute a “commercial item” as defined at 48 C.F.R. § 2.101, consisting of “commercial computer software” and “commercial computer software documentation” under 48 C.F.R. § 12.212. Accordingly, if Client is an agency of the U.S. Government or any contractor therefore, Client only receives those rights with respect to the SaaS Services and Documentation as are granted to all other end users in accordance with (a)48 C.F.R. § 227.7201 through 48 C.F.R. § 227.7204, with respect to the Department of Defense and their contractors, or (b) 48 C.F.R. § 12.212, with respect to all other U.S. Government agencies, users and their contractors.

(j) Equitable Relief. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 6 or, in the case of Client, Section 2(c), would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and agrees that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including a restraining order, an injunction, specific performance and any other relief that may be available from any court, without any requirement to post a bond or other security, or to prove actual damages or that monetary damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity or otherwise.

(k) Counterparts; Electronic Execution. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. This Agreement may be executed in electronic form (or signed and scanned into electronic form) and shall be just as valid and enforceable as any original wet-ink signed version thereof.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the Effective Date.

Approved and Accepted By:

Interpersonal Frequency LLC	CLIENT
By: 	By: _____
Harish R. Rao, CEO	AUTHORIZED USER
Title: CEO	Title: _____
Date: 10/11/2022	Date: _____

EXHIBIT A: STATEMENT OF WORK

Will be attached separately.

EXHIBIT D: PREMIER SERVICE LEVEL AGREEMENT; SUPPORT & MAINTENANCE TERMS

This Service Level Agreement is integrated into and made a part of the Agreement and outlines the level of service that I.F. will provide in the event of outages, standard maintenance, scheduled maintenance and other issues with Client's hosted website.

Interpersonal Frequency (I.F.) will provide Client with our Fulcrum cloud server based SaaS hosting, managed Drupal (version 7, 8, or 9) CMS, necessary technical and support infrastructure, and the service levels detailed on the following pages, for a single website (or websites defined in Exhibit A). Domain Name Services (DNS), domain name registration fees, and security certificates for encrypted communication are not included (with the exception of LetsEncrypt.org automated certificates provisioned by I.F.). Additional websites or sub-domains not specified in Exhibit A are excluded and will be removed or suspended if detected unless previously authorized by I.F. in writing.

Fulcrum Cloud Services: Managed Hosting with Drupal CMS Care

The following sections cover Standard Maintenance, Scheduled Maintenance and Emergency Maintenance of the SaaS Services. With certain exceptions described below, each of these forms of maintenance are included with your Fulcrum SaaS subscription over the period specified.

Standard Maintenance

This is routine and necessary maintenance that is done in a way that does not interfere with Client's normal web server operations. This type of maintenance is done on a regular basis. I.F. prioritizes such maintenance based on Client's needs each month and may include:

- examining and rotating server and web log files
- checking automated backups, both of the site & database(s)
- applying standard operating system security patches
- applying standard operating system bug fixes
- applying infrastructure layer patches (PHP, cache, db, etc.)
- applying standard Drupal core CMS security updates
- applying standard Drupal module security updates
- disabling unused accounts, such as those unused for more than 60 days.

In the event there are critical patches that affect our operational security, either at the operating system level or at the Drupal CMS level, I.F. may elect to patch those components through our standard maintenance process at any time in our discretion. However, these are typically part of our Scheduled Maintenance (see below). Standard maintenance covers application and database issues. Backups are done automatically, with a typical minimum of one backup per day (and hourly on the production database).

I.F.follows best practices for installing maintenance updates regularly on the test/staging server first before "pushing" these updates to the live servers. I.F. may request Client to review updates on the testing environment prior to going live. We reserve the right to deploy these types of patches without Client review.

Scheduled Maintenance: Covered by Separate I.F. Support Plan

Scheduled Maintenance is a higher level of maintenance, where I.F. engineers make preventive or corrective modifications to the configuration of the server or web applications (e.g., Drupal CMS). SCHEDULED MAINTENANCE AS DESCRIBED BELOW IS NOT INCLUDED IN OUR FULCRUM SAAS SUBSCRIPTION. Scheduled maintenance is often part of an (optional) I.F. support plan. In any event, YOU ARE REQUIRED TO PERFORM (OR ALLOW TO BE PERFORMED) SCHEDULED MAINTENANCE, including but not limited to the tasks below. Failure to do so means we may suspend your service to ensure overall system integrity or security.

Tasks include, but are not limited to:

- applying Drupal CMS module updates
- applying Drupal minor version upgrades (e.g., Drupal 8.1 to Drupal 8.2)
- applying patches to custom software / applications, including custom Drupal Modules and third-party applications
- upgrading server software packages, including major “dot releases” (e.g., significant PHP version upgrades)
- major modifications to cloud server configuration (e.g., adding RAM/memory)
- major modifications to the operating system

Because such maintenance tasks are inherently riskier, these tasks are normally scheduled to occur outside of regular operating hours (see below). I.F. normally provides at least two days’ notice to affected clients for Scheduled Maintenance. Such maintenance down time does not count against our uptime guarantee. This policy exists to protect our client’s interests and the integrity of the software and hardware installation. A client may request that scheduled maintenance occur during business hours if the maintenance is specific to the client or on a Fulcrum dedicated subscription; if this is requested, we require our clients to submit a notice via our support intake system to confirm, as this is outside of I.F.’s policy. I.F. reserves the right to conduct scheduled maintenance at any time, in its discretion, should overall system stability be threatened.

Emergency Maintenance

Emergency Maintenance is performed by I.F. engineers in the event of a “Critical-High-Urgent” emergency, see definition under Response Time Goals section below. There are two types of emergencies: controllable and uncontrollable.

- Controllable emergencies are emergencies where our client commits an error that is largely preventable. Examples of such errors include but are not limited to bypassing restrictions of the CMS; client engineers performing code updates that were not tested and/or not operating from the “Clients Who Code” instructions; uploading very large files that are not optimized for the web; DNS changes made without at least two (2) advance day notification to I.F.; or denying the installation of a required security patch; errors caused by third-party APIs.
- Uncontrollable emergencies are emergencies that are largely out of the control of either the client or I.F., such as a break in internet connectivity or Distributed Denial-of-Service condition.

Both types of emergencies are covered by I.F. SLA response times (see below).

Hours of Operation

Interpersonal Frequency uses servers and resources solely in the continental United States of America, except for any Content Delivery Network (CDN) we may provide. The client is required to contact I.F. via authorized means for the response time commitments to apply: via the support intake system or toll-free phone number with a logged ticket. I.F. representatives will respond to non-critical client requests for support within 1 hour during business hours, and by 9 a.m. ET the next business day for non-critical requests submitted outside of business hours. See our response time goals below. Business hours for I.F. are Monday - Friday, excluding Federal holidays, 9am ET - 5pm ET for our U.S. clients based in the Eastern or Central time zones, and 9am – 5pm PT for customers in the Mountain or Pacific time zones.

Getting Support for Fulcrum SaaS or for I.F. Support Plans

In order to obtain support, an authorized contact must request support via the support intake system (preferred) or, in an emergency, call toll-free 844-311-iFiF. You must always first make use of our dedicated toll-free telephone number and/or support intake system prior to calling any individual I.F. employees for our SLA commitments to apply. We make use of ticket tracking software to assist in tracking service requests. I.F. will release information and perform work requested to only to designated, pre-authorized individuals at each client. It is the client's responsibility to update I.F. with the correct authorized users, to include email address and mobile numbers, by having an existing authorized contact email I.F. support at the address above with any changes.

Uptime Commitment and Exclusions

Subject to the provisions of Section 3 (as to our Cloud Provider) and the other terms and conditions of the Agreement, our goal is for our SaaS hosting environment to provide an uptime of 99.95% for public (anonymous) site users and 99.9% for content editors/administrators on a rolling ninety-day basis. These guarantees exclude any Cloud Provider exclusions plus the following conditions:

- Scheduled maintenance;
- Issues caused by user error or by client-specific third-party integrations including controllable emergencies (see definition below);
- Denial-of-Service (DoS) conditions. DoS is defined as a condition where total inbound bandwidth to our CDN (if applicable) or Fulcrum origin servers unexpectedly (i.e., without notifying I.F. support 24 hours in advance) exceeds 120% of the previous 30-days' 90th percentile bandwidth, measured in Gbps;
- DoS-like conditions caused by a customer's unauthorized or inadvertent actions, including but not limited to penetration testing of Fulcrum systems ("pentesting") or other customer error such as excessive queries by an external service or insufficient operating limits of a Client-provided Third-Party service;
- External conditions which exceed normal and allocated operating limit;
- DNS (domain name server) issues, including customer DNS downtime;
- Previously unauthorized testing, scanning, port-scanning, and client security testing; you must notify I.F. one week (5 business days) in advance to conduct such testing, and such

testing is subject to I.F. Cloud Provider and I.F. approval at its sole discretion.

I.F. shall have the right, in its sole discretion, to ban IP addresses and/or restrict traffic in order to maintain system stability if any of the above are detected or if the Cloud Provider takes any other remedial actions permitted under its terms of service. Our uptime commitment is only in effect if payment(s) for hosting are up-to-date. Optional Apache Solr or Elasticsearch service which may be included in your Premier Fulcrum hosting are excluded from our uptime commitment.

Emergency Service Conditions

This Agreement includes the following levels of emergency service:

- Uncontrollable emergencies: Subject to any constraints or limitations imposed by our Cloud Provider, I.F. will work to mitigate or fix any issues caused by increased traffic, denial-of-service attack, or other server or network based issues as quickly as possible. There is no additional charge above the standard monthly fee agreement so long as these issues are not caused by any change from the client or its contractors who have been authorized to work on Fulcrum Cloud Services or-related third party systems.
- Controllable emergencies: Subject to any constraints or limitations imposed by our Cloud Provider, a controllable emergency is any issue that could be corrected through the regular management admin interface and related web based interfaces available to the client. This includes, but is not limited to, issues that could be corrected by un-publishing content due to formatting issues, poorly formatted database queries caused by non-I.F. engineers on database(s), programming errors introduced by the client or by third-party tools and APIs integrated with the clients' website, or site usage/bandwidth exceeding allocated amounts (defined below), and unavailability relating to malware, viruses, Trojan horses, and/or malicious code that was introduced by the client directly or indirectly, and client DNS outage or usage of the site as a file server.

I.F. technicians will respond to "Critical/High/Urgent" emergencies (see definitions under "Response Time Goals" section below) issues within 1 (one) hour during regular business hours. You must notify us if you detect an issue via the modes identified in the earlier "Getting Support for Fulcrum SaaS or for I.F. Support Plans" section for our response times to apply. I.F. strives to respond more quickly than these time frames; these are our minimum commitments. I.F. engineers will determine if an outage or issue is an uncontrollable or controllable emergency based on overall hosting system availability for all I.F. clients; if no other clients are experiencing related or similar issues, we will preliminarily judge the issue to be "controllable." In any case, our first priority is to resolve any critical or emergency issues. After resolution, I.F. will perform a "root cause" analysis, which will provide information on why the failure occurred and how to prevent it in the future. If necessary, the root cause analysis will also judge the critical or emergency issue as "controllable" or "uncontrollable."

Response Time Goals

Criticality	Description	Response Time	Resolution Time Objective
Critical - High - Urgent	The production environment is unavailable for a large number of anonymous users or authenticated users or the Client's business operations are severely impacted with no available workaround.	Under 1 hour	1 hour
Medium	The production environment is operating but an issue is causing disruption of business operations and any workarounds are insufficient; dev/testing/train environment are severely degraded affecting authenticated user access (e.g., content authors, developers).	1 hour during business hours; 2 hours otherwise	4 business hours
Low	All environments are operating, but the issue is inconveniencing a minority of public or authenticated users	2 hours during business hours; next business morning otherwise	5 business days

The above service response times and Recovery Time Objectives are our commitments, subject only to any constraints or limitations imposed by our Cloud Provider. I.F. makes every commercially reasonable effort to respond and resolve issues as quickly as possible. In general, we can respond to most Critical systems issues within five minutes.

During weekends, US Federal holidays, and evening hours, an emergency response fee of $500 will be charged per incident and added to your hosting invoice should the incident be deemed a controllable emergency. This is in addition to any regular fees you pay for hosting. There is no charge (above the standard fee) for non-emergency issues responded to during normal business hours.

Escalation: In case of any kind of emergency issue that causes an outage, we automatically escalate to a supervising engineer after one hour (or faster if no relevant issues are seen). If the senior engineer cannot find the cause after one hour, it will be escalated to the network provider and, if necessary, the Cloud Provider.

Monitoring: I.F. uses commercially reasonable means to monitor our Cloud Services performance and Client site status. IT IS YOUR RESPONSIBILITY TO REPORT ISSUES TO I.F. VIA THE PREVIOUSLY DEFINED EMAIL AND/OR PHONE NUMBER FOR OUR SERVICE COMMITMENTS TO APPLY. These systems automatically notify us of many possible issues. We reserve the right to deactivate or discontinue the use of any/all I.F. monitoring or alarms caused by intermittent issues unresolved by the Client, including Client DNS issues or API-limit issues causing throttling of Client-provided Third Party Services, at any time and suspend our uptime guarantee until such issues are remediated by the Client to the satisfaction of I.F, in its sole

judgment.

Service Credit

I.F. strives to ensure that all the web properties we manage are accessible at all times. There are circumstances, both in and outside of our control that may cause interruptions of service. Our systems are monitored 24 hours a day through automated systems continuously, and our technicians are paged immediately upon any monitoring alerts. Should we be alerted to a problem, we will begin work during business hours and continue to work beyond regular business hours with no extra charge to Client. In the unlikely event that we are unable to meet our response time guarantee or our server uptime guarantee for reasons within our control (excluding those caused by Cloud Provider), I.F. will credit a pro rata amount. The amount of proration will be based on the formula: (Fulcrum Managed Cloud Hosting Yearly Fee) / 12 (i.e., number of months in a year) = amount of Service Credit. The Service Credit will exclude any fee paid for non-Fulcrum items (e.g., Drupal Support hours/tickets, if applicable, the pro rata bundled cost of a Voice of Citizen® subscription, CDN subscription). This service credit will be issued against a subsequent hosting invoice (e.g., the next quarter or year depending on your billing setup). If the issue is an uncontrollable emergency and we fail to respond in within our Response Time, we will also not assess any emergency response fee. We will measure the total time of failure using our internal monitoring system. One such service credit is available per each one-year subscription period.

Infrastructure, Scaling, and Redundancy

We provide redundancy through I.F. and the Cloud Provider's architecture, and both I.F. and the Cloud Provider each maintain automated tools to facilitate recovery where redundancy is not feasible. We engage Cloud Providers with a cloud server footprint in multiple data centers to facilitate restoration in the event of a datacenter-level failure. We urge you to use redundant providers for upstream services like DNS which Fulcrum Cloud Services rely upon.

Database and File size

Client website's (database and files) are limited in space (detailed in the Fulcrum hosting quote you will receive and/or in Exhibit A Statement of Work). Client will be notified if more space is required and billed for at then prevailing rates. The maximum file size permitted on our Fulcrum Cloud Services is 256MB; we recommend files no larger than 15MB hosted on our systems for optimal performance. Some clients will receive the (optional, extra fee) Fulcrum Large File Uploads feature; for such clients, the maximum file size permitted is 5GB.

Page Views & Bandwidth

Web hosting includes up to a defined maximum per month (see your Fulcrum hosting quote or Exhibit A Statement of Work), and consistent overage in page views will require additional hosting fees. In addition, total bandwidth transfer to Fulcrum origin servers is limited to 2TB (both inbound and outbound) each month. Our optional CDN/WAF/DDoS Third-Party service has virtually unlimited bandwidth for public / anonymous users included. We reserve the right to manage traffic across our upstream networks to protect our operations, including restricting traffic and/or IPs. VIDEOS ARE NOT ALLOWED TO BE HOSTED DIRECTLY ON OUR FULCRUM ARCHITECTURE; WE REQUIRE OUR CLIENTS TO USE A THIRD PARTY SERVICE (E.G., YOUTUBE) FOR VIDEO FILES. Should peak usage conditions require I.F. to horizontally or vertically scale origin server resources, I.F. will provision necessary resources to protect system integrity and invoice the Client at our cost + 20%.

Backups

Fulcrum automatically makes encrypted hourly backups of content, and encrypted daily backups of file information and code repositories on production ("live") systems. Data restoration requests must be made to I.F. support via email and will be prioritized accordingly. Excessive requests (beyond one such request per calendar month) shall be billed at the then-prevalent DevOps engineering rate per quarter-hour thereof. Non-production environment backups (e.g., for development, testing, or training servers) are done daily. The client can elect to make and download a backup at any time in any environment via Fulcrum GUI. You may download any backup at any time to your own systems. Retention of backups from production and other environments is on a rolling 7-day basis, with the oldest backups automatically deleted. Clients may elect, contingent on an extra fee, for the Fulcrum 6 Month backup retention feature. For such clients, one (1) weekly backup is preserved each week for 6 Months, on a rolling basis, and beyond the normal 7-day basis retention.

Infrastructure

The collective infrastructure of I.F. and its Cloud Provider provides burst capacity to millions of anonymous users, which will be able to handle the typical traffic on the client's website. The hosting fee includes security updates for the Drupal CMS but not major/minor revision upgrades (e.g., Drupal version 7 to Drupal version 8). Such upgrades are handled via an optional I.F. support plan if desired. Our fee does include I.F. or Cloud Provider hosting infrastructure upgrades (e.g., hardware, operating system, etc.) as needed. I.F. reserves the right to adjust cache times (i.e., content publishing cache) to ensure client site operability.

Voice of Patron®/Voice of Citizen® SaaS analytics service

Premier SLA customers may receive a subscription to our Voice of Patron® (for public libraries) or Voice of Citizen® (for civic government) service, with semi-annual reporting (i.e., two (2) reports per year) and insights collection, included with their Fulcrum SaaS subscription. This technology collects analytics about your web users via an active (survey)-based system and passive (behavioral/clickstream) system. Please see related Privacy Policy and Terms of Service.

Drupal Support from our Solutions Engineering Team

In addition to Drupal CMS Care, which is a part of our Fulcrum SaaS services, we may provide you with an I.F. Support contract. Support Contract tickets/hours are separate from Drupal CMS maintenance services. However, you will contact the I.F. Solutions Engineering Team through our support intake system as you would for Fulcrum-related questions. Drupal Support contract response times are different than Fulcrum cloud services response times and negotiated separately as part of your Support contract.

This Service Level Agreement (SLA) is subject to change at any time, in our discretion, and such changes or amendments will automatically apply to the Agreement and to this Exhibit D.

Disaster Recovery

I.F. provides superior service level guarantees on network uptime, infrastructure availability and server failure replacements, subject to the terms of use of our Cloud Provider. These high level service commitments are augmented with a high- availability backup placed in a separate data center of the Cloud Provider.

Network Outage Scenario

In the event of a prolonged network outage does not prevent us from, and at Client's written request, I.F. will move the client web site / systems to another facility. The website and data will be recovered from the most recent available known-good backup of the site, and moved to a separate hosting provider once the new infrastructure has been made available to I.F. engineers. Migration to the new Cloud Provider or alternative facility will be agreed upon between County and Contractor and hours deducted from the I.F. Evolution and Support plan.

Severe Cloud Server or Infrastructure Failure Scenario

In the event of a severe server or infrastructure failure whereupon the client's website or applications are rendered unreachable, subject to any constraints or limitations imposed by our Cloud Provider, I.F. will restore the clients' website from the most recent "good" backup upon provisioning by I.F. of new servers. This will be done at no additional charge to the client so long as it is not the result of a controllable emergency issue, as defined above.

Data Center Disaster Scenario

In the unlikely event of a natural or man-made disaster that disables the entire data facility within which our clients' website(s) reside, subject to any constraints or limitations imposed by our Cloud Provider, I.F. will restore the client's web site, at the client's request, to an unaffected data center, assuming that the backup is recoverable from the affected data facility. (I.F. standard policy is to have one backup of a client's website and data in a physically separate facility from the main facility.) Migration to a new Cloud Provider or Cloud Provider hosting facility will be billed at then-current I.F. billing rates, and the hosting costs of the new servers are the responsibility of the client. The client's website may be restored from a backup to a secondary Cloud Provider site at no charge.

Security for Fulcrum Cloud Services & SaaS Services

Fulcrum is designed specifically as an enterprise government Drupal web platform and uses a security first approach. Subject to the terms of use of our Cloud Provider, Fulcrum provides a secure platform where I.F. customers may develop and maintain highly-available, secure websites. Subject to the terms of use of our Cloud Provider, I.F. manages, monitors, and secures the environment where our customer websites run including the operating system and LEMP (Linux, Nginx, MySQL, PHP) stack and network layers. Additionally, I.F. provides tools to manage this system.

Subject to the terms of use of our Cloud Provider, I.F. will protect our customers' Drupal installation with secure infrastructure, appropriately configured access to resources, and industry-leading best practices around updates and managing data. Fulcrum will provide:

- Docker-container based architecture, wherein every component is isolated and treated from a least-trust model where possible
- Denial of Service Protection via Third-Party product DDoS protection, WAF, and Amazon AWS load balancer/IP means
- Automated security monitoring on the Fulcrum origin servers
- HTTPS with End-to-end encryption (the client is responsible for providing security certificate(s) unless LetsEncrypt.org service is used, as recommended)
- IP-whitelisting via Fulcrum Zuul, Fulcrum Streamlined Whitelist (FSW) and optional

MFA (multi-factor access)
- Role-based permissions
- Automated encrypted backup and retention, including hourly backups of production environment database (Note: restoration requires a support ticket to I.F. support)
- Secure code and database access via version control and other means (Note: I.F. does not provide direct database access to Fulcrum SaaS Services)
- Secure Cloud Provider data centers that are SOC 2 Type II and/or ISO 27001 certified; optional GovCloud FISMA/FedRamp environment available though not recommended for I.F. non-U.S. Government customers).

The architecture is run as though no single component can be trusted by ensuring isolation between components. The Fulcrum infrastructure is built on a container-based architecture (Docker), which can be run in both the public cloud (AWS) as well as a private cloud environment (e.g., the clients' Tier 1 data center). Containers allow partitioning into isolated areas where individual applications (e.g., web server, Varnish cache, etc.) can run virtually independently. The Fulcrum infrastructure isolates resources while making it simple to scale and deploy updates across the entire infrastructure readily. We support encryption including TLS. The Fulcrum architecture uses the Amazon Aurora distributed file system in the cloud, leveraging either Amazon's Elastic File Store (EFS), or when configured in a client data center, GlusterFS bricks. Database services are also clustered, using Amazon's Aurora distributed database service (in the cloud) or MariaDB Galera Cluster in a client data center. Resources are accessed over encrypted channels using client-server authentication. Fulcrum core infrastructure will never be directly accessible by the public (and its BGP origin protected) by our optional CDN/WAF/DDoS service. This means that DDoS and other types of router-based attacks more difficult. All of these features combined together is why we (in conjunction with our Cloud Provider) can offer a 99.95% public uptime (must select optional CDN/WAF/DDoS service).

Security Monitoring & Network Intrusion Protection

I.F. runs a multitude of automated and other checks in real time of its Fulcrum cloud-hosted environment, made available to our DevOps team via the Amazon Cloudwatch service. These systems allow logging and auditing of activities via monitoring tools like New Relic. I.F. uses AWS security groups and public/private key as the only way a Fulcrum admin can access a server for administration level access (command line access). Traffic is tunneled to origin servers, preventing circumvention of request validation, filtering, and caching. The public/private key security infrastructure runs for any services available from our Fulcrum GUI, Fulcrum Deploy, and Fulcrum Hinge workflow. At the container layer, our infrastructure detects and prevents unauthorized host access. Our logging infrastructure records the identity of blocked accounts for later investigation. Security logs from the servers are collected and analyzed.

Denial of Service Protection

I.F. works with Amazon (or other Cloud Provider) and Third-Party CDN/WAF/DDoS product (if selected) to provide management of denial-of-service attacks, filtering ongoing attacks and isolating traffic streams through Cloud Provider load balancers for each production (live) site and the production environment. Our CDN/WAF/DDoS services (which are optional) include BGP origin protection, making it challenging for public users to uncover the Fulcrum origin IPs. Fulcrum is designed from the ground-up to mitigate malicious bot attacks. Our solution's optional CDN/WAF/DDoS provides significant protections against Botnet attacks (layer 3, 4, and 7 OSI-model attacks), as well as BGP origin protection. I.F. and its Cloud Provider defend, host

and defend some of the largest government customers in the United States. We are confident of providing you a highly available platform should you select our Fulcrum with CDN/WAF/DDoS Cloud Services.

Data Center Security

I.F.'s primary data centers are with Amazon Web Services (AWS), which provides 24/7 direct support on any issue. Access to data centers is granted though both keycard and biometric scanning protocols and protected by round-the-clock surveillance monitoring. Every AWS data center employee undergoes a thorough background security check before hiring. The I.F. team does not have access to physical servers except those that may be provided by a client at a DR facility should you so choose (which is not a standard part of Fulcrum Cloud Services).

I.F. Employee Administrative Access

We grant access according to least privilege. Authorized employees can interact with servers via a secure system without terminal access—and if they must, SSH-key based authentication is used (no direct SSH to Fulcrum SaaS is possible; a bastion server is used). All I.F. DevOps and Drupal engineering employees, including the core team and Drupal Solutions Engineers, have undergone rigorous background checks. Our team is chosen and trained specifically for the needs of security conscious U.S.-based government customers.

Releasing Patches and Updates

I.F. and its Cloud Provider manage each dedicated Fulcrum instance for large customers individually, including the patch and update schedule. I.F. and its Cloud Provider continually deploys new container and upgrades to the infrastructure in the background, including the latest supported kernel, OS, and packages. Containers are migrated to the updated instances automatically and the older systems are retired. I.F. uses Ansible & Chef to help automate server changes, update containers, and prevent human errors on system updates and configuration changes. Core CMS application updates and security patches are tested internally by the dedicated I.F. Drupal Solutions Engineering team before the client's staff is asked to verify; once verification is complete, you authorize the release to production (of Drupal application updates). We and our Cloud Provider reserve the right to deploy system and application patches to protect the integrity of the system at will. We will make reasonable efforts to seek your approval prior to patch deployment.

Interpersonal Frequency Privacy Policy Effective: 9/1/2018

This Privacy Policy explains how information is collected, used and disclosed by Interpersonal Frequency (I.F.) with respect to the access and use of our systems and our SaaS services, including our Fulcrum Cloud Services and Voice of Citizen®/Voice of Patron® analytics and Aggregated Statistics. This Privacy Policy does not apply to any third-party websites, services or applications that you may access by or through our services and we advise you, as our Client, to review this Privacy Policy and implement any conforming changes in your own website Privacy Policy and/or user agreements.

FOR THE AVOIDANCE OF DOUBT, INTERPERSONAL FREQUENCY DISCLAIMS ANY AND ALL RESPONSIBILITY FOR THE TERMS AND CONDITIONS OF CLIENT'S PRIVACY, ONLINE COOKIE AND OTHER DATA PRIVACY AND PROTECTION POLICIES AND PROCEDURES (INCLUDING USER OPT-IN OR OPT-OUT FUNCTIONALITIES) APPLICABLE TO CLIENT'S WEB SITE AND/OR ANY OTHER PRODUCTS OR SERVICES, EVEN IF SUCH PRODUCTS OR SERVICES ARE ACCESSED OR USED BY OR THROUGH OUR SERVICES. WE ARE NOT IN A POSITION TO, AND OUR SERVICES DO NOT INCLUDE, ANY FORM OF PRIVACY IMPACT REPORT OR DATA PROTECTION IMPACT ASSESSMENT INVOLVING CLIENT'S BUSINESS, ITS OPERATIONS, ITS USER BASE AND/OR ITS MARKETING PRACTICES. NEVERTHELESS, I.F. WILL BE PLEASED TO COLLABORATE WITH CLIENT ON ANY OF THESE ISSUES OR CONSIDERATIONS ON SUCH TERMS AS MUTUALLY AGREED OUTSIDE THESE TERMS OR OUR AGREEMENT.

Information We Collect

Non-Personally-Identifying Information

Like most website operators, I.F. collects non-personally-identifying information of the sort that web browsers and servers typically make available, such as (but not limited to) the browser type, language preference, referring site, and the date and time of each visitor request. Depending on your service level (and specifically, if you are using the Voice of Citizen®/Patron® analytics platform), we may also collect information on behaviors of our clients' end users; for example, what links or pages they are visiting and how much time they spend on a page. The purpose in collecting non-personally identifying information is to better understand how our clients' web users utilize the website. We only collect such behavioral data with authorization from our client.

From time to time, I.F. may release non-personally-identifying information in the aggregate, e.g., by publishing a report on trends in the usage of its clients websites. You may choose to opt-out of participation in such aggregation. If you select to opt-out of participation in data-aggregation/benchmarking, and in fairness to our other clients, you will not be provided certain benchmark data about your website performance in comparison to others. I.F. also collects information like Internet Protocol (IP) addresses. I.F. does not use such information to identify its visitors, however, and does not disclose such information, other than under the circumstances described below.

Personally-Identifying Information

Certain visitors to I.F.'s websites choose to interact with I.F. Cloud Services & SaaS Services in ways that require I.F. to gather personally-identifying information (PII). The amount and type of information that I.F. gathers depends on the nature of the interaction. I.F. collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with I.F. or, more often, its Client's end users. I.F. does not disclose personally-identifying information other than as described below. Visitors can always refuse to

supply personally-identifying information, with the caveat that it may prevent them from engaging in certain website-related activities. We do not knowingly collect personal information from children. If we learn that we have collected personal information of a child under 13, we will take steps to delete such information as soon as possible. We also provide our clients with methods to reduce the amount of PII collected; for example, through the use of an “exclude” tag in data submission or data display fields.

Information Collected for Others

Through our services our clients can collect information about how their end users use their websites and certain third-party applications, as well as how those websites and applications are performing. Our technology also provides diagnostic predictions based on sophisticated machine learning algorithms. Our clients determine the types of data and information that is sent to I.F. for collection and analysis. The collection of this data and information by our clients is subject to their own privacy policy.

Because our clients have discretion to determine what data and information is collected about or from their users, our Privacy Policy does not apply to any end user data that we may collect, obtain, or access in connection with operating our services on behalf of our clients. We ask that our clients abide by all applicable laws, rules and regulations, including laws relating to privacy and data collection and post an online privacy policy that provides users with clear notice of its practices regarding data collection, use, and disclosure, however, we have no control over our clients’ activities or the disclosures they make in their privacy policy.

We may analyze end user data and information in the aggregate for purposes of internal research and/or to determine overall trends or metrics concerning how users are engaging with websites and may report such general trends publicly, without disclosing any specific end user data and information.

Cookies

Cookies are strings of information, generally a small text file that web browsers place on a web visitor’s computer. I.F. makes use of cookies only for customers using our optional Voice of Citizen/Patron service. I.F. does not make use of cookies for its non-Voice of Citizen/Patron web hosting customers unless it is necessary for client-initiated diagnostic test purposes. In the event of cookie usage, I.F. uses both session-based and persistent cookies. Session cookies exist only during one session, and disappear when you close your browser. Persistent cookies remain on your computer after you close your browser or turn off your computer. Most internet browsers automatically accept cookies. However, you can instruct your browser, by editing its options, to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

How We Share the Information We Collect With Others

I.F. will not share personally-identifiable information about you to anyone, unless you instruct us to do so or if we notify you that the information you provide will be shared in a particular manner and you provide such information. If you are a Client of I.F. and have provided your email address, I.F. may occasionally send you an email to tell you about new features, solicit your feedback, or just keep you up to date with what’s going on with I.F. and our products.

I.F. may disclose non-personally-identifying and personally-identifying information to its employees, contractors and affiliated organizations that (i) need to know that information in order to process it on I.F.’s behalf or to provide services available through I.F., and (ii) that have agreed not to disclose it to others. Some of those employees, contractors and affiliated organizations may be located outside of your home country; by using I.F.’s website and services, you consent to the transfer of such information to them.

Other than to its employees, contractors and affiliated organizations, as described above, I.F. discloses personally-identifying information only when (or if we believe we are) required to do so by law, or when I.F. believes in good faith that disclosure is reasonably necessary to protect the property or rights of I.F., third parties or the public at large. I.F. may also transfer and/or provide information about you in connection with an acquisition, sale of company assets, or other situation where customer and user information would be transferred as one of I.F. business assets.

We will share the data and information we collect for our clients with that organization. We do not share any specific end user data or information with individuals or with other companies, other than with the specific customer whose website transmitted the data and information to us. We may share information about our clients and their end users in anonymous and/or aggregated form with third parties for industry analysis, demographic profiling, research, analysis and other similar purposes.

How to Access Your Information

Please contact the I.F. support via the I.F. support intake system to access your information or to contact an I.F. Research Analyst. Information will only be provided to Authorized Users.

Security Measures We Take to Protect Your Information

I.F. and its Cloud Provider employ administrative, physical and electronic measures designed to protect your information from unauthorized access, however, despite these efforts, no security measures are perfect or impenetrable and no method of data transmission can be guaranteed against any interception or other type of misuse. We and our Cloud Provider use standard industry practices to help prevent unauthorized use of, access to or alteration of visitor and user information and hosted data. These practices include the appropriate use of firewalls, HTTPS encryption, limiting storage of financial information to a PCI compliant third party provider (if applicable to you), system redundancies, and hosting at a 24/7 secured, controlled environment. In the event that your personal information is compromised as a result of a breach of security, we will promptly notify you if your personal information has been compromised, as required by applicable law.

Privacy Policy Is Subject to change

Any information that is collected is subject to our Privacy Policy in effect at the time such information is collected. I.F. may modify and revise its Privacy Policy from time to time. If we make any material changes to this policy, we will notify you of such changes by emailing a link to the updated privacy policy to the primary Authorized User on file for your account at least thirty (30) days prior to the change(s) taking effect. Your continued use of our services after any change in this Privacy Policy becomes effective will constitute your acceptance of such change(s).

Exhibit E: Terms of Service for Voice of Citizen® and/or Voice of Patron® SaaS

Effective: September 1, 2018

The following terms and conditions (the "Terms"), which are hereby incorporated into and made a part of our Agreement, govern the use of the services made available through Interpersonal Frequency's Voice of Citizen® (for our municipal and state government as well as not-for-profit customers) and/or Voice of Patron® service (for our library customers) (collectively, our "Services"), which are provided to Client ("you") subject to your compliance with these Terms and any other operating rules, policies and procedures (including, without limitation, I.F. Privacy Policy and Security Policy) set forth in our Agreement or published from time to time by Interpersonal Frequency. By accessing and/or using our Services, you are agreeing to be bound by these Terms and our Agreement, which constitute a binding legal agreement between us. In some cases, your use of certain services may be subject to additional terms, which will be presented to you when you sign up to use or engage in those services.

Voice of Citizen® / Voice of Patron® Service

I.F. provides predictive analytics tools for collecting website survey (qualitative) and behavioral (quantitative) data for improving citizen (and/or patron) experience on our customer's websites. Our Services may change from time to time, or we may stop (permanently or temporarily) providing our Services (or any features therein) to you or to users generally. We reserve the right to create limits on access and use of the Services in our sole discretion.

We may make available certain software to install on your website(s) in order to access and use our Services. As long as you comply with these Terms and our Agreement, you have the right to install and use our software to access and use the Services for your own website(s). This non-exclusive, limited license, which may be terminated by I.F. at any time in its discretion, is for the sole purpose of enabling you to use the Services in the manner permitted by these Terms and our Agreement during the term thereof. You may not copy, modify, derive, distribute, sell, or lease our software or any part of our Services or included software, nor may you reverse engineer or attempt to extract the source code of our software, unless you have our written permission. Subject to the foregoing license, all right, title and interest in and to our software and Services is retained by Interpersonal Frequency.

Acceptable Use Policies

Use of the Services

You are responsible for your use of the Services and you agree that you will only use our Services in compliance with these Terms and our Agreement and all applicable laws and regulations.
Privacy

OUR PRIVACY POLICY IS FOR YOUR BENEFIT AND IS NOT DESIGNED TO APPLY DIRECTLY TO YOUR OWN WEB SITE OR TO YOUR RELATIONSHIP WITH YOUR USERS (INCLUDING AUTHORIZED USERS). YOU AGREE TO PUBLISH AND ABIDE BY AN APPROPRIATE PRIVACY POLICY (AND COOKIE POLICY) THAT ADEQUATELY AND TRANSPARENTLY DESCRIBES YOUR COLLECTION, USE, STORAGE AND SHARING OF ANY INFORMATION YOU COLLECT FROM THE USERS OF YOUR WEBSITE(S) USING THE SERVICES BASED ON WHATEVER LAWS AND REGULATIONS MAY APPLY TO YOU AND TO YOUR USE. YOU FURTHER AGREE TO COMPLY WITH ALL APPLICABLE LAWS RELATING TO YOUR COLLECTION, USE AND SHARING OF THE INFORMATION YOU COLLECT FROM

USERS OF YOUR WEBSITE USING THE SERVICES. YOUWILL NOT (AND WILL NOT ALLOW ANY THIRD PARTY TO) USE OUR SERVICES TO TRACK OR COLLECT PERSONALLY IDENTIFIABLE INFORMATION OR PERSONAL DATA OF USERS WITHOUT PROPERLY INFORMING YOUR USERS OF YOUR SPECIFIC DATA COLLECTION PRACTICES AND MEETING ALL OTHER APPLICABLE LAWS AND REGULATIONS.

Enforcement

Without limiting any other remedies, I.F. has the right (though not the obligation) to, in I.F.'s sole discretion (i) refuse Services to or remove anything that, in I.F.'s reasonable opinion, violates any I.F.policy or is in any way harmful or objectionable, or (ii) terminate or deny access to and use of the Services to any individual or entity for any reason, in I.F.'s sole discretion.

Unauthorized Activities

You may not do any of the following while using or accessing the Services:

- attempt to access the Services or download content from the Services through the use of any engine, software, scraping tool, agent, device or mechanism other than the software provided by us;
- access, tamper with, or use non-public areas of the Services, our computer systems, or the technical delivery systems of our providers;
- use the Services for the benefit of any third party or in any manner not permitted by these Terms or our Agreement;
- violate any applicable law or regulation; or
- encourage or enable someone to do any of the foregoing.

We reserve the right to access, read, preserve and disclose any information provided through the Services we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce this Agreement, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of I.F., our users and the public.

Your Representations

You represent and warrant that (i) you have the necessary power and authority to enter into these Terms and our Agreement (if you are agreeing to these terms on behalf of your employer or other entity, you represent and warrant that you have full legal authority to bind your employer or such entity to these Terms and our Agreement) and (ii) your use of the Services will be in strict accordance with these Terms and our Agreement, the I.F. Privacy Policy, the applicable Acceptable Use Policy and all applicable laws and regulations (including without limitation any local laws or regulations in your country regarding online conduct and acceptable content and/or the transfer of personal data to the United States from the country in which you reside) and will not infringe, violate or misappropriate the rights of any Party, user or third party.

Termination of Services for Voice of Citizen® and/or Voice of Patron® SaaS

You can terminate your Service and these Terms (without termination of our Agreement) at any time by removing our software code from your website(s) or by providing notice of termination of these Terms to us. We reserve the right to terminate or suspend your access to any or all portions of the Services at any time, for any reason, including your violation or breach of any of these Terms or out Agreement. Upon any such termination, all rights and licenses granted to you in these Terms (and in our discretion our Agreement) immediately end. If your account or access to our Services is terminated or suspended because you violated these Terms or our Agreement, you will not be entitled to any refund of any fees nor will any fees be credited or reimbursed to

you in any form and you will have no further right to access any of the foregoing.

Refund Policy for Voice of Citizen® and/or Voice of Patron® SaaS

There will be no refunds or credits for partial periods of service or refunds for months unused, nor can we append "unused service" to your account should you wish to reactivate in the future.

Information and Intellectual Property Rights for Voice of Citizen® and/or Voice of Patron® SaaS

I.F. may retain and use, subject to the terms of its Privacy Policy, information collected in your use of the Services (other than Client Data that continues to identify you). I.F. will not share information associated with you or your website with any third parties unless I.F. (i) has your permission; (ii) concludes that it is required by law or has a good faith belief that access, preservation or disclosure of such information is reasonably necessary to protect the rights, property or safety of I.F., our users or the public; or (iii) provides such information in anonymous or aggregated form that does not identify you.

Our Services and our Site are protected by copyright, trademark, and other laws of the United States and foreign countries. I.F. and its licensors exclusively own all right, title and interest in and to the Services, including all associated intellectual property rights. You may not remove, alter or obscure any copyright, trademark, service mark or other proprietary rights notices incorporated in or accompanying the Services or the Site. All rights not granted to you under this Agreement are reserved by and to Interpersonal Frequency for itself and its licensors.

Attachment H
Health Insurance Portability and Accountability Act (HIPAA)
Business Associate Requirements

DEFINITIONS

Terms used, but not otherwise defined, in this Schedule shall have the same meaning as those terms are defined in 45 Code of Federal Regulations (CFR) sections 160.103, 164.304, and 164.501. All regulatory references in this Schedule are to Title 45 of the Code of Federal Regulations unless otherwise specified.

a. ***Business Associate.*** "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the parties to this agreement shall mean Contractor.
b. ***Covered Entity.*** "Covered entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement shall mean County.
c. **HIPAA Rules**. "HIPAA rules" shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR part 160 and part 164, as amended and supplemented by Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009.
d. ***Designated Record Set***. "Designated Record Set" shall have the same meaning as the term "designated record set" in Section 164.501.
e. ***Electronic Protected Health Information***. "Electronic Protected Health Information" (EPHI) means individually identifiable health information that is transmitted or maintained in electronic media; it is limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.
f. ***Individual***. "Individual" shall have the same meaning as the term "individual" in Section 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).
g. ***Privacy Rule***. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
h. ***Protected Health Information***. "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in Section 160.103 and is limited to the information created or received by Business Associate from or on behalf of County.
i. ***Required By Law***. "Required by law" shall have the same meaning as the term "required by law" in Section 164.103.
j. ***Secretary***. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.
k. ***Breach***. The acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule that compromises the security or privacy of the PHI and subject to the exclusions set forth in Section 164.402. Unless an exception applies, an impermissible use or disclosure of PHI *is presumed* to be a breach, unless it can be demonstrated there is a low

probability that the PHI has been compromised based upon, at minimum, a four-part risk assessment:

1. Nature and extent of PHI included, identifiers and likelihood of re-identification;
2. Identity of the unauthorized person or to whom impermissible disclosure was made;
3. Whether PHI was actually viewed or only the opportunity to do so existed;
4. The extent to which the risk has been mitigated.

l. ***Security Rule***. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

m. ***Unsecured PHI.*** "Unsecured PHI" is protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in relevant HHS guidance.

n. ***Security Incident***. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. "Security Incident" includes all incidents that constitute breaches of unsecured protected health information.

OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE

a. Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as required by law.
b. Business Associate agrees to use appropriate safeguards to comply with Subpart C of 45 CFR part 164 with respect to EPHI and PHI, and to prevent the use or disclosure of the Protected Health Information other than as provided for by this Agreement.
c. Business Associate agrees to make uses and disclosures requests for Protected Health Information consistent with minimum necessary policy and procedures.
d. Business Associate may not use or disclose protected health information in a manner that would violate subpart E of 45 CFR part 164.504 if used or disclosed by Covered Entity.
e. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
f. Business Associate agrees to report to County any use or disclosure of Protected Health Information not authorized by this Agreement.
g. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of County, agrees to adhere to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
h. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of County, and in the time and manner designated by County, to Protected Health Information in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under Section 164.524.

i. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the County directs or agrees to make pursuant to Section 164.526 at the request of County or an Individual, and in the time and manner designed by County.
j. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of County, available to the County at the request of County or the Secretary, in a time and manner designated by the County or the Secretary, for purposes of the Secretary determining County's compliance with the Privacy Rule.
k. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for County to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.
l. Business Associate agrees to provide to County or an Individual in the time and manner designated by County, information collected in accordance with Section (k) of this Schedule, in order to permit County to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.
m. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of County.
n. Business Associate shall conform to generally accepted system security principles and the requirements of the final HIPAA rule pertaining to the security of health information.
o. Business Associate shall ensure that any agent to whom it provides EPHI, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect such EPHI.
p. Business Associate shall report to County any Security Incident within three (3) business days of becoming aware of such incident. Business Associate shall also facilitate breach notification(s) to the appropriate governing body (i.e. HHS, OCR, etc.) as required by law. As appropriate and after consulting with County, Business Associate shall also notify affected individuals and the media of a qualifying breach.
q. Business Associate understands that it is directly liable under the HIPAA rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of Protected Health Information that are not authorized by this Attachment, the underlying contract as or required by law.

PERMITTED USES AND DISCLOSURES BY CONTRACTOR AS BUSINESS ASSOCIATE

Except as otherwise limited in this Schedule, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement; provided that such use or disclosure would not violate the Privacy Rule if done by County.

OBLIGATIONS OF COUNTY

a. County shall provide Business Associate with the notice of privacy practices that County produces in accordance with Section 164.520, as well as any changes to such notice.
b. County shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.
c. County shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that County has agreed to in accordance with Section 164.522.

PERMISSIBLE REQUESTS BY COUNTY

County shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if so requested by County, unless the Business Associate will use or disclose Protected Health Information for, and if the Agreement provides for, data aggregation or management and administrative activities of Business Associate.

DUTIES UPON TERMINATION OF AGREEMENT

a. Upon termination of the Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from County, or created, maintained, or received by Business Associate on behalf of County, that Business Associate still maintains in any form. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
b. In the event that Business Associate determines that returning or destroying Protected Health Information is infeasible, Business Associate shall provide to County notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of the Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protection Health Information.

MISCELLANEOUS

a. **Regulatory References**. A reference in this Schedule to a section in the HIPAA Privacy Rule means the section as in effect or as amended, and for which compliance is required.
b. **Amendment**. The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.

c. **Survival**. The respective rights and obligations of Business Associate under this Schedule shall survive the termination of the Agreement.
d. **Interpretation**. Any ambiguity in this Schedule shall be resolved in favor of a meaning that permits County to comply with the Privacy Rule.
e. **Reservation of Right to Monitor Activities**. County reserves the right to monitor the security policies and procedures of Business Associate.

Attachment IP
Intellectual Property Rights

1. The County of San Mateo ("County"), shall and does own all titles, rights and interests in all Work Products created by Contractor and its subcontractors (collectively "Vendors") for the County under this Agreement. Contractor may not sell, transfer, or permit the use of any Work Products without the express written consent of the County.

2. "Work Products" are defined as all materials, tangible or not, created in whatever medium pursuant to this Agreement, including without limitation publications, promotional or educational materials, reports, manuals, specifications, drawings and sketches, computer programs, software and databases, schematics, marks, logos, graphic designs, notes, matters and combinations thereof, and all forms of intellectual property.

3. Contractor shall not dispute or contest, directly or indirectly, the County's exclusive right and title to the Work Products nor the validity of the intellectual property embodied therein. Contractor hereby assigns, and if later required by the County, shall assign to the County all titles, rights and interests in all Work Products. Contractor shall cooperate and cause subcontractors to cooperate in perfecting County's titles, rights or interests in any Work Product, including prompt execution of documents as presented by the County.

4. To the extent any of the Work Products may be protected by U.S. Copyright laws, Parties agree that the County commissions Vendors to create the copyrightable Work Products, which are intended to be work-made-for-hire for the sole benefit of the County and the copyright of which is vested in the County.

5. In the event that the title, rights, and/or interests in any Work Products are deemed not to be "work-made-for-hire" or not owned by the County, Contractor hereby assigns and shall require all persons performing work pursuant to this Agreement, including its subcontractors, to assign to the County all titles, rights, interests, and/or copyrights in such Work Product. Should such assignment and/or transfer become necessary or if at any time the County requests cooperation of Contractor to perfect the County's titles, rights or interests in any Work Product, Contractor agrees to promptly execute and to obtain execution of any documents (including assignments) required to perfect the titles, rights, and interests of the County in the Work Products with no additional charges to the County beyond that identified in this Agreement or subsequent change orders. The County, however, shall pay all filing fees required for the assignment, transfer, recording, and/or application.

6. Contractor agrees that before commencement of any subcontract work it will incorporate this **ATTACHMENT IP** to contractually bind or otherwise oblige its subcontractors and personnel performing work under this Agreement such that the County's titles, rights, and interests in Work Products are preserved and protected as intended herein.