STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: LS3752

Starting Date: 11/15/2023

Expiration Date: 9/14/2026

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and CitizenLab (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

One year renewal option, new expiration date 9/14/2027.

Effective Date of Amendment: 3/11/2026

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

Signed by:
Sarah Horton
3DE05EA6E21841D...

3/26/2026

Contractor's Signature — Date

Sarah Horton

Contractor's Name (Print)

Director, North America

Title (Print)

STATE OF UTAH

DocuSigned by:
C38BE9DAC528424...

3/30/2026

Director, State of Utah Division of Purchasing — Date

For Division of Purchasing Internal Use			
Purchasing Agent	Phone #	E-mail Address	**Contract #**
Laurel deLagerheim	801-957-7121	ldelagerheim@utah.gov	LS3752

Contract #: LS3752

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

CitizenLab
Name

2093 Philadelphia Pike
Street Address

Claymont	Delaware	19703
City	*State*	*Zip*

Vendor # N/A Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation Contact

Name: *Sarah Horton* *Phone Number:* +1 707-227-9834 *Email:* *sarah.horton*@citizenlab.co

2. CONTRACT PORTFOLIO NAME: Customer Engagement.
3. GENERAL PURPOSE OF CONTRACT: Citizen Engagement Platform.
4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2021, Solicitation# KM21-47
5. CONTRACT PERIOD: Effective Date: 11/15/23 . Termination Date: 9/14/26 unless terminated early or extended in accordance with the terms and conditions of this contract.
6. Administrative Fee (if any): One Quarter of One Percent (or 0.25%).
7. Prompt Payment Discount Details (if any): None.
8. ATTACHMENT A: NASPO ValuePoint Master Agreement Terms and Conditions ATTACHMENT B: Scope of Work
ATTACHMENT C: Price Schedule
ATTACHMENT D: End User License Agreements
Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.
9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #KM21-47.
10. Each person signing this Agreement represents and warrants that he/she is duly authorized and has legal capacity to execute and deliver this Agreement and bind the parties hereto. Each signatory represents and warrants to the other that the execution and delivery of the Agreement and the performance of each party's obligations hereunder have been duly authorized and that the Agreement is a valid and legal agreement binding on the parties and enforceable in accordance with its terms.
IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Contractor's signature	Date
	Nov 28, 2023

Sarah Horton, Director of North America, CitizenLab
Type or Print Name and Title

DIVISION OF PURCHASING

DocuSigned by:
C38BE9DAC528424...

Director, Division of Purchasing	Date
	11/29/2023

ATTACHMENT A

NASPO VALUEPOINT MASTER AGREEMENT TERMS AND CONDITIONS

I. Definitions

1.1 **Acceptance** means acceptance of goods and services as set forth in Section IX of this Master Agreement.

1.2 **Contractor** means a party to this Master Agreement, whether a person or entity, that delivers goods or performs services under the terms set forth in this Master Agreement.

1.3 **Embedded Software** means one or more software applications which permanently reside on a computing device.

1.4 **Intellectual Property** means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

1.5 **Lead State** means the State centrally administering any resulting Master Agreement(s) who is a party to this Master Agreement.

1.6 **Master Agreement** or **Contract** means the underlying agreement executed by and between the Lead State, acting in cooperation with NASPO ValuePoint, and the Contractor, as now or hereafter amended.

1.7 **NASPO ValuePoint** is a division of the National Association of State Procurement Officials ("NASPO"), a 501(c)(3) limited liability company. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and may perform contract administration functions relating to collecting and receiving reports, as well as other contract administration functions as assigned by the Lead State.

1.8 **Order** or **Purchase Order** means any purchase order, sales order, contract or other document used by a Purchasing Entity to order the Products.

1.9 **Participating Addendum** means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any additional Participating Entity-specific language or other requirements (*e.g.*, ordering procedures specific to the Participating Entity, entity-specific terms and conditions, etc.).

1.10 **Participating Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states properly authorized to enter into a Participating Addendum, that has executed a Participating Addendum.

1.11 **Participating State** means a state that has executed a Participating Addendum or has indicated an intent to execute a Participating Addendum.

1.12 **Product** or **Products and Services** means any equipment, software (including embedded software), documentation, service, or other deliverable supplied or created by the Contractor pursuant to this Master Agreement. The term Product includes goods and services.

1.13 **Purchasing Entity** means a state (as well as the District of Columbia and US territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states if authorized by a Participating Addendum, that issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

II. Term of Master Agreement

2.1 **Initial Term.** The initial term of this Master Agreement is for Five (5) years, beginning when the first master agreement under this portfolio is signed. The term of this Master Agreement may be amended beyond the initial term for two (2) additional years at the Lead State's discretion and by mutual agreement and upon review of requirements of Participating Entities, current market conditions, and Contractor performance.

2.2 **Amendment Limitations.** The terms of this Master Agreement will not be waived, altered, modified, supplemented, or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.

2.3 **Amendment Term.** The term of the Master Agreement may be amended past the initial term and stated renewal periods for a reasonable period if in the judgment of the Lead State a follow-on competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection will not be deemed to limit the authority of a Lead State under its state law to otherwise negotiate contract extensions.

III. Order of Precedence

3.1 Order. Any Order placed under this Master Agreement will consist of the following documents:

3.1.1 A Participating Entity's Participating Addendum ("PA");

3.1.2 NASPO ValuePoint Master Agreement, including all attachments thereto;

3.1.3 A Purchase Order or Scope of Work/Specifications issued against the Master Agreement;

3.1.4 The Solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions;

3.1.5 Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State.

3.2 Conflict. These documents will be read to be consistent and complementary. Any conflict among these documents will be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

3.3 Participating Addenda. Participating Addenda will not be construed to diminish, modify, or otherwise derogate any provisions in this Master Agreement between the Lead State and Contractor. Participating Addenda will not include a term of agreement that exceeds the term of the Master Agreement.

IV. Participants and Scope

4.1 Requirement for a Participating Addendum. Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed.

4.2 Applicability of Master Agreement. NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum, subject to Section III. For the purposes of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering

document (*e.g.*, purchase order or contract) used by the Purchasing Entity to place the Order.

4.3 Authorized Use. Use of specific NASPO ValuePoint Master Agreements by state agencies, political subdivisions and other Participating Entities is subject to applicable state law and the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

4.4 Obligated Entities. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Participating Entities incur no financial obligations on behalf of other Purchasing Entities.

4.5 Notice of Participating Addendum. Contractor shall email a fully executed PDF copy of each Participating Addendum to pa@naspovaluepoint.org to support documentation of participation and posting in appropriate databases.

4.6 Eligibility for a Participating Addendum. Eligible entities who are not states may under some circumstances sign their own Participating Addendum, subject to the consent of the Chief Procurement Official of the state where the entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists; the entity must ensure that they have the requisite procurement authority to execute a Participating Addendum.

4.7 Prohibition on Resale. Subject to any specific conditions included in the solicitation or Contractor's proposal as accepted by the Lead State, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products purchased under this Master Agreement. Absent any such condition or explicit permission, this limitation does not prohibit: payments by employees of a Purchasing Entity for Products; sales of Products to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

4.8 Individual Customers. Except as may otherwise be agreed to by the Purchasing Entity and Contractor, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement and as the Participating Entity has in the Participating Addendum, including but

not limited to any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

4.9 Release of Information. Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan.

4.10 No Representations. The Contractor shall not make any representations of NASPO ValuePoint, the Lead State, any Participating Entity, or any Purchasing Entity's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent.

V. NASPO ValuePoint Provisions

5.1 Applicability. NASPO ValuePoint is not a party to the Master Agreement. The terms set forth in Section V are for the benefit of NASPO ValuePoint as a third-party beneficiary of this Master Agreement.

5.2 Administrative Fees

5.2.1 NASPO ValuePoint Fee. Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee must be submitted quarterly and is based on all sales of products and services under the Master Agreement (less any charges for taxes or shipping). The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with a vendor's response to the Lead State's solicitation.

5.2.2 State Imposed Fees. Some states may require an additional fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee rate or amount, payment method and schedule for such reports and payments will be incorporated into the applicable Participating Addendum. Unless agreed to in writing by the state, Contractor may not adjust the Master Agreement pricing to include the state fee for purchases made by Purchasing Entities within the jurisdiction of the state. No such agreement will affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by Purchasing Entities outside the jurisdiction of the state requesting the additional fee.

5.3 NASPO ValuePoint Summary and Detailed Usage Reports

5.3.1 Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. All sales made under this Master Agreement must be reported as cumulative totals by state. Contractor must submit a report for each quarter, including quarters during which a Contractor has no sales, in which case this will be indicated in the Reporting Tool. Reports must be submitted no later than thirty (30) days following the end of the calendar quarter (as specified in the reporting tool).

5.3.2 Detailed Sales Data. Contractor shall also report detailed sales data in accordance with the instructions in Attachment J.1 and in the format set forth in Attachment J, or as otherwise instructed by NASPO ValuePoint. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports must be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports must include sales information for all sales under Participating Addenda executed under this Master Agreement.

5.3.3 Reporting on Personal Use. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity ((state and agency, city, county, school district, etc.) under whose authority the employee is purchasing Product for personal use and the amount of sales. No personal identification numbers (*e.g.*, names, addresses, social security numbers or any other numerical identifier) may be submitted with any report.

5.3.4 Executive Summary. Contractor shall, upon request, provide NASPO ValuePoint cooperative contract coordinator with an executive summary that includes, at a minimum and for the preceding quarter, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any Participating Addendum roll out or implementation activities and issues. NASPO ValuePoint cooperative contract coordinator and Contractor will determine the format and content of the executive summary.

5.3.5 Use of Data. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports will have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

5.4 NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review

5.4.1 Staff Education. Contractor shall work cooperatively with NASPO ValuePoint personnel. Contractor shall present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the master agreement and participating addendum process, and the manner in which eligible entities can participate in the Master Agreement.

5.4.2 Onboarding Plan. Upon request by NASPO ValuePoint, Contractor shall, as Participating Addendums are executed, provide plans to launch the program for the Participating Entity. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the scope and terms of the Master Agreement as available to the Participating Entity and eligible Purchasing Entities.

5.4.3 Annual Contract Performance Review. Contractor shall participate in an annual contract performance review with the Lead State and NASPO ValuePoint, which may at the discretion of the Lead State be held in person and which may include a discussion of marketing action plans, target strategies, marketing materials, Contractor reporting, and timeliness of payment of administration fees.

5.4.4 Use of NASPO ValuePoint Logo. The NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a separate logo use agreement is executed with NASPO ValuePoint.

5.4.5 Most Favored Customer. Contractor shall, within thirty (30) days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-party contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this Master Agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

5.5 **Cancellation.** In consultation with NASPO ValuePoint, the Lead State may, in its discretion, cancel the Master Agreement pursuant to section 28, or not exercise an option to renew, when utilization of Contractor's Master Agreement does not warrant further administration of the Master Agreement. The Lead State may also exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. Cancellation based on nonuse or under-utilization will not occur sooner than [two years] after execution of the Master Agreement. This subsection does not limit the discretionary right of either the Lead State or Contractor to cancel the Master Agreement or terminate for default subject to the terms herein. This subsection also does not limit any right of the Lead State to cancel the Master Agreement under applicable laws.

VI. Pricing, Payment & Leasing

6.1 **Pricing.** The prices contained in this Master Agreement or offered under this Master Agreement represent the not-to-exceed price to any Purchasing Entity.

6.1.1 All prices and rates must minimally be guaranteed for the first year of the Master Agreement.

6.1.2 Following the first year of the Master Agreement, any request for a price or rate adjustment must be for an equal guarantee period and must be made at least thirty (30) days prior to the effective date.

6.1.3 Requests for a price or rate adjustment must include sufficient documentation supporting the request. Any adjustment or amendment to the Master Agreement will not be effective unless approved in writing by the Lead State.

6.1.4 No retroactive adjustments to prices or rates will be allowed.

6.2 **Payment.** Unless otherwise agreed upon in a Participating Addendum or Order, Payment after Acceptance will be made within thirty (30) days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance, unless a different late payment amount is specified in a Participating Addendum or Order, or otherwise prescribed by applicable law. Payments will be remitted in the manner specified in the Participating Addendum or Order. Payments may be made via a purchasing card with no additional charge.

6.3 **Leasing or Alternative Financing Methods**. The procurement and other applicable laws of some Purchasing Entities may permit the use of leasing

or alternative financing methods for the acquisition of Products under this Master Agreement. Where the terms and conditions are not otherwise prescribed in an applicable Participating Addendum, the terms and conditions for leasing or alternative financing methods are subject to negotiation between the Contractor and Purchasing Entity.

VII. Ordering

7.1 Order Numbers. Master Agreement order and purchase order numbers must be clearly shown on all acknowledgments, packing slips, invoices, and on all correspondence.

7.2 Quotes. Purchasing Entities may define entity-specific or project-specific requirements and informally complete the requirement among companies having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity's rules and policies. The Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost, and other factors considered.

7.3 Applicable Rules. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

7.4 Required Documentation. Contractor shall not begin work without a valid Purchase Order or other appropriate commitment document under the law of the Purchasing Entity.

7.5 Term of Purchase. Orders may be placed consistent with the terms of this Master Agreement and applicable Participating Addendum during the term of the Master Agreement and Participating Addendum.

7.5.1 Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement.

7.5.2 Notwithstanding the previous, Orders must also comply with the terms of the applicable Participating Addendum, which may further restrict the period during which Orders may be placed or delivered.

7.5.3 Financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

7.5.4 Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor shall perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration, cancellation, or termination of this Master Agreement, or in any manner inconsistent with this Master Agreement's terms.

7.5.5 Orders for any separate indefinite quantity, task order, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

7.6 Order Form Requirements. All Orders pursuant to this Master Agreement, at a minimum, must include:

7.6.1 The services or supplies being delivered;

7.6.2 A shipping address and other delivery requirements, if any;

7.6.3 A billing address;

7.6.4 Purchasing Entity contact information;

7.6.5 Pricing consistent with this Master Agreement and applicable Participating Addendum and as may be adjusted by agreement of the Purchasing Entity and Contractor;

7.6.6 A not-to-exceed total for the products or services being ordered; and

7.6.7 The Master Agreement number or the applicable Participating Addendum number, provided the Participating Addendum references the Master Agreement number.

7.7 Communication. All communications concerning administration of Orders placed must be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

7.8 Contract Provisions for Orders Utilizing Federal Funds. Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this Master Agreement.

VIII. Shipping and Delivery

8.1 Shipping Terms. All deliveries will be F.O.B. destination, freight pre-paid, with all transportation and handling charges paid by the Contractor.

8.1.1 Notwithstanding the above, responsibility and liability for loss or damage will remain the Contractor's until final inspection and acceptance when responsibility will pass to the Purchasing Entity except as to latent defects, fraud, and Contractor's warranty obligations.

8.2 Minimum Shipping. The minimum shipment amount, if any, must be contained in the Master Agreement. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an Order to be shipped without transportation charges that is back ordered will be shipped without charge.

8.3 Inside Deliveries. To the extent applicable, all deliveries will be "Inside Deliveries" as designated by a representative of the Purchasing Entity placing the Order. Inside Delivery refers to a delivery to a location other than a loading dock, front lobby, or reception area. Specific delivery instructions will be noted on the order form or Purchase Order. Costs to repair any damage to the building interior (*e.g.*, scratched walls, damage to the freight elevator, etc.) caused by Contractor or Contractor's carrier will be the responsibility of the Contractor. Immediately upon becoming aware of such damage, Contractor shall notify the Purchasing Entity placing the Order.

8.4 Packaging. All products must be delivered in the manufacturer's standard package. Costs must include all packing and/or crating charges. Cases must be of durable construction, in good condition, properly labeled and suitable in every respect for storage and handling of contents. Each shipping carton must be marked with the commodity, brand, quantity, item code number and the Purchasing Entity's Purchase Order number.

IX. Inspection and Acceptance

9.1 Laws and Regulations. Any and all Products offered and furnished must comply fully with all applicable Federal, State, and local laws and regulations.

9.2 Applicability. Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section IX will apply. This section is not intended to limit rights and remedies under the applicable commercial code.

9.3 Inspection. All Products are subject to inspection at reasonable times and places before Acceptance. Contractor shall provide right of access to the Lead State, or to any other authorized agent or official of the Lead State or other Participating or Purchasing Entity, at reasonable times, to monitor

and evaluate performance, compliance, and/or quality assurance requirements under this Master Agreement.

9.3.1 Products that do not meet specifications may be rejected. Failure to reject upon receipt, however, does not relieve the contractor of liability for material (nonconformity that substantially impairs value) latent or hidden defects subsequently revealed when goods are put to use.

9.3.2 Acceptance of such goods may be revoked in accordance with the provisions of the applicable commercial code, and the Contractor is liable for any resulting expense incurred by the Purchasing Entity related to the preparation and shipping of Product rejected and returned, or for which Acceptance is revoked.

9.4 Failure to Conform. If any services do not conform to contract requirements, the Purchasing Entity may require the Contractor to perform the services again in conformity with contract requirements, at no increase in Order amount. When defects cannot be corrected by re-performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements and reduce the contract price to reflect the reduced value of services performed.

9.5 Acceptance Testing. Purchasing Entity may establish a process, in keeping with industry standards, to ascertain whether the Product meets the standard of performance or specifications prior to Acceptance by the Purchasing Entity.

9.5.1 The Acceptance Testing period will be thirty (30) calendar days, unless otherwise specified, starting from the day after the Product is delivered or, if installed by Contractor, the day after the Product is installed and Contractor certifies that the Product is ready for Acceptance Testing.

9.5.2 If the Product does not meet the standard of performance or specifications during the initial period of Acceptance Testing, Purchasing Entity may, at its discretion, continue Acceptance Testing on a day-to-day basis until the standard of performance is met.

9.5.3 Upon rejection, the Contractor will have fifteen (15) calendar days to cure. If after the cure period, the Product still has not met the standard of performance or specifications, the Purchasing Entity may, at its option: (a) declare Contractor to be in breach and terminate the Order; (b) demand replacement Product from Contractor at no additional cost to Purchasing Entity; or, (c) continue the cure period for an additional time period agreed upon by the Purchasing Entity and the Contractor.

9.5.4 Contractor shall pay all costs related to the preparation and shipping of Product returned pursuant to the section.

9.5.5 No Product will be deemed Accepted and no charges will be paid until the standard of performance or specification is met.

X. Warranty

10.1 Applicability. Unless otherwise specified in the Master Agreement, Participating Addendum, or ordering document, the terms of this Section X will apply.

10.2 Warranty. The Contractor warrants for a period of one year from the date of Acceptance that: (a) the Product performs according to all specific claims that the Contractor made in its response to the solicitation, (b) the Product is suitable for the ordinary purposes for which such Product is used, (c) the Product is suitable for any special purposes identified in the solicitation or for which the Purchasing Entity has relied on the Contractor's skill or judgment, (d) the Product is designed and manufactured in a commercially reasonable manner, and (e) the Product is free of defects.

10.3 Breach of Warranty. Upon breach of the warranty set forth above, the Contractor will repair or replace (at no charge to the Purchasing Entity) the Product whose nonconformance is discovered and made known to the Contractor. If the repaired and/or replaced Product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made.

10.4 Rights Reserved. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity, including, without limitation, actual damages, and, as applicable and awarded under the law, to a prevailing party, reasonable attorneys' fees and costs.

10.5 Warranty Period Start Date. The warranty period will begin upon Acceptance, as set forth in Section IX.

XI. Product Title

11.1 Conveyance of Title. Upon Acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Product free and clear of all liens, encumbrances, or other security interests.

11.2 Embedded Software. Transfer of title to the Product must include an irrevocable and perpetual license to use any Embedded Software in the Product. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title. A subsequent transfer of this software license will be at no additional cost or charge to either Purchasing Entity or Purchasing Entity's transferee.

11.3 License of Pre-Existing Intellectual Property. Contractor grants to the Purchasing Entity a nonexclusive, perpetual, royalty-free, irrevocable, license to use, publish, translate, reproduce, transfer with any sale of tangible media or Product, perform, display, and dispose of the Intellectual Property, and its derivatives, used or delivered under this Master Agreement, but not created under it ("Pre-existing Intellectual Property"). The Contractor shall be responsible for ensuring that this license is consistent with any third-party rights in the Pre-existing Intellectual Property.

XII. Indemnification

12.1 General Indemnification. CitizenLab shall hold NASPO harmless from liability to third parties resulting from infringement by the Service of any patent or any copyright or misappropriation of any trade secret, provided CitizenLab is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement; CitizenLab will not be responsible for any settlement it does not approve in writing. The foregoing obligations do not apply with respect to portions or components of the Service (i) not supplied by CitizenLab, (ii) made in whole or in part in accordance with NASPO specifications, (iii) that are modified after delivery by CitizenLab, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where NASPO continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where NASPO's use of the Service is not strictly in accordance with this Agreement. If, due to a claim of infringement, the Services are held by a court of competent jurisdiction to be or are believed by CitizenLab to be infringing, CitizenLab may, at its option and expense (a) replace or modify the Service to be non-infringing provided that such modification or replacement contains substantially similar features and functionality, (b) obtain for NASPO a license to continue using the Service, or (c) if neither of the foregoing is commercially practicable, terminate this Agreement and NASPO's rights hereunder and provide NASPO a refund of any prepaid, unused fees for the Service.

12.2 Intellectual Property Indemnification. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers and employees ("Indemnified Party"), from and against claims, damages

or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use infringes the patent or copyright, or misappropriates any trade secret, of another person or entity ("Intellectual Property Claim").

12.2.1 The Contractor's obligations under this section will not extend to infringement directly caused by:

12.2.1.1 Contractor's compliance with nonstandard specifications provided by Purchasing Entity;

12.2.1.2 any unauthorized modification of the Product by Purchasing Entity after delivery;

12.2.1.3 continuation of the allegedly infringing activity by Purchasing Entity after being notified thereof or after being directed to make modifications that would have avoided the alleged infringement; and

12.2.1.4 any combination of the Product with any other product, system or method, unless the Product, system or method is:

12.2.1.4.1 provided by the Contractor or the Contractor's subsidiaries or affiliates;

12.2.1.4.2 specified by the Contractor to work with the Product;

12.2.1.4.3 reasonably required to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

12.2.1.4.4 reasonably expected to be used in combination with the Product.

12.2.2 The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of the Intellectual Property Claim. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible.

12.2.3 The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of the Intellectual Property Claim and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim.

12.2.4 If the Product is held by a court of competent jurisdiction to be infringing, or is believed by CitizenLab to be infringing, CitizenLab shall, at its option and expense (a) replace or modify the Service to be non-infringing provided that such modification or replacement contains substantially similar features and functionality, (b) obtain for NASPO a license to continue using the Product, or (c) if neither of the foregoing is commercially practicable, terminate Purchasing Entity's right to use the Product and refund to Purchasing Entity any prepaid fees for the Product. The foregoing shall be in addition to and not exclusive of any other remedies provided to Purchasing Entity by law.

12.2.5 Unless otherwise set forth herein, Section 12.2 is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

XIII. Insurance

13.1 Term. Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. A Participating Entity may negotiate alternative Insurance requirements in their Participating Addendum.

13.2 Class. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

13.3 Coverage. Coverage must be written on an occurrence basis. The minimum acceptable limits will be as indicated below:

13.3.1 Contractor shall maintain Commercial General Liability insurance covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising

liability, and property damage, with a limit of not less than $1 million per occurrence and $2 million general aggregate;

13.3.2 Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

13.4 Notice of Cancellation. Contractor shall pay premiums on all insurance policies. Contractor shall provide notice to a Participating Entity who is a state within five (5) business days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.

13.5 Notice of Endorsement. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) provides that written notice of cancellation will be delivered in accordance with the policy provisions, and (2) provides that the Contractor's liability insurance policy will be primary, with any liability insurance of any Participating State as secondary and noncontributory.

13.6 Participating Entities. Contractor shall provide to Participating States and Participating Entities the same insurance obligations and documentation as those specified in Section XIII, except the endorsement is provided to the applicable Participating State or Participating Entity.

13.7 Furnishing of Certificates. Contractor shall furnish to the Lead State copies of certificates of all required insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance will be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. Failure to provide evidence of coverage may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

13.8 Disclaimer. Insurance coverage and limits will not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

XIV. General Provisions

14.1 Records Administration and Audit

14.1.1 The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and Orders placed by Purchasing Entities under it to the extent and in such detail as will adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government

(including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right will survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Master Agreement, whichever is later, or such longer period as is required by the Purchasing Entity's state statutes, to assure compliance with the terms hereof or to evaluate performance hereunder.

14.1.2 Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or Orders or underpayment of fees found as a result of the examination of the Contractor's records.

14.1.3 The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement that requires the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

14.2 Confidentiality, Non-Disclosure, and Injunctive Relief

14.2.1 **Confidentiality.** Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity or Purchasing Entity's clients.

14.2.1.1 Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity ("Confidential Information").

14.2.1.2 Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information.

14.2.1.3 Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity; or (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

14.2.2 Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement.

14.2.2.1 Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information.

14.2.2.2 Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person.

14.2.2.3 Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing

Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information.

14.2.2.4 Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits, and evidence of the performance of this Master Agreement.

14.2.3 **Injunctive Relief.** Contractor acknowledges that Contractor's breach of Section 14.2 would cause irreparable injury to the Purchasing Entity that cannot be inadequately compensated in monetary damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

14.2.4 **Purchasing Entity Law.** These provisions will be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

14.2.5 **NASPO ValuePoint.** The rights granted to Purchasing Entities and Contractor's obligations under this section will also extend to NASPO ValuePoint's Confidential Information, including but not limited to Participating Addenda, Orders or transaction data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line-item descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead State, a Participating State, or any governmental entity exercising an audit, inspection, or examination pursuant to this Master Agreement. To the extent permitted by law, Contractor shall notify the Lead State of the identify of any entity seeking access to the Confidential Information described in this subsection.

14.2.6 **Public Information.** This Master Agreement and all related documents are subject to disclosure pursuant to the Lead State's public information laws.

14.3 Assignment/Subcontracts

14.3.1 Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

14.3.2 The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties, to NASPO ValuePoint and other third parties.

14.4 Changes in Contractor Representation. The Contractor must, within ten (10) calendar days, notify the Lead State in writing of any changes in the Contractor's key administrative personnel managing the Master Agreement. The Lead State reserves the right to approve or reject changes in key personnel, as identified in the Contractor's proposal. The Contractor shall propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

14.5 Independent Contractor. Contractor is an independent contractor. Contractor has no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and shall not to hold itself out as agent except as expressly set forth herein or as expressly set forth in an applicable Participating Addendum or Order.

14.6 Cancellation. Unless otherwise set forth herein, this Master Agreement may be canceled by either party upon sixty (60) days' written notice prior to the effective date of the cancellation. Further, any Participating Entity may cancel its participation upon thirty (30) days' written notice, unless otherwise limited or stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision will not affect the rights and obligations attending Orders outstanding at the time of cancellation, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit. Cancellation of the Master Agreement due to Contractor default may be immediate.

14.7 Force Majeure. Neither party to this Master Agreement shall be held responsible for delay or default caused by fire, riot, unusually severe weather, other acts of God, or acts of war which are beyond that party's reasonable control. The Lead State may terminate this Master Agreement upon determining such delay or default will reasonably prevent successful performance of the Master Agreement.

14.8 Defaults and Remedies

14.8.1 The occurrence of any of the following events will be an event of default under this Master Agreement:

14.8.1.1 Nonperformance of contractual requirements;

14.8.1.2 A material breach of any term or condition of this Master Agreement;

14.8.1.3 Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading;

14.8.1.4 Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

14.8.1.5 Any default specified in another section of this Master Agreement.

14.8.2 Upon the occurrence of an event of default, the Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of fifteen (15) calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure will not diminish or eliminate Contractor's liability for damages, including liquidated damages to the extent provided for under this Master Agreement.

14.8.3 If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and the Lead State shall have the right to exercise any or all of the following remedies:

14.8.3.1 Any remedy provided by law;

14.8.3.2 Termination of this Master Agreement and any related Contracts or portions thereof;

14.8.3.3 Assessment of liquidated damages as provided in this Master Agreement;

14.8.3.4 Suspension of Contractor from being able to respond to future bid solicitations;

14.8.3.5 Suspension of Contractor's performance; and

14.8.3.6 Withholding of payment until the default is remedied.

14.8.4 Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and shall have all of the rights and

remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Unless otherwise specified in an Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions will be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

14.9 Waiver of Breach. Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies will not operate as a waiver under this Master Agreement, any Participating Addendum, or any Purchase Order. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order will not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, any Participating Addendum, or any Purchase Order.

14.10 Debarment. The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in public procurement or contracting by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

14.11 No Waiver of Sovereign Immunity

14.11.1 In no event will this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

14.11.2 This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This

section is also not a waiver by the state of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

14.12 Governing Law and Venue

14.12.1 The procurement, evaluation, and award of the Master Agreement will be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award will be governed by the law of the state serving as Lead State. The construction and effect of any Participating Addendum or Order against the Master Agreement will be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's state.

14.12.2 Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the state serving as Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement will be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum will be in the Purchasing Entity's state.

14.12.3 If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; a Participating State if a named party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

14.13 Assignment of Antitrust Rights. Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

   Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

   a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

   b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

   c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

   d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

   e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or

employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:**

   a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

   b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

   c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. **Personal Data Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

   a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in

accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. **Notification of Legal Requests**: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. **Termination and Suspension of Service**:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:** Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:** The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. **Data Center Audit**: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

    Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

    No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

    Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Right to Remove Individuals:** The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. **Compliance with Accessibility Standards**: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. **Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. **Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. **Subscription Terms**: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

    No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, CITIZENLAB AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CITIZENLABS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND CITIZENLAB'S REASONABLE CONTROL; OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID BY NASPO TO CITIZENLAB FOR THE SERVICES UNDER THIS AGREEMENT IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT CITIZENLAB HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

   Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

   a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

   b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

   c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

   d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

   e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or

employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:** The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

    a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

    b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

    c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

    a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

    b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

    c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. **Notification of Legal Requests**: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. **Termination and Suspension of Service**:

    a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its

digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:**

   a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

   b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. **Data Center Audit**: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

    Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

    No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Compliance with Accessibility Standards**: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the

Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity.

20. **Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. **Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. **Subscription Terms:** Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

    No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

    NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY OF A PERSON, CITIZENLAB AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL EQUIPMENT AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CITIZENLABS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY OR CORRUPTION OF DATA OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES;
    (C) FOR ANY MATTER BEYOND CITIZENLAB'S REASONABLE CONTROL; OR (D) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID BY NASPO TO CITIZENLAB FOR THE SERVICES UNDER THIS AGREEMENT IN THE 12 MONTHS PRIOR TO THE ACT THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT CITIZENLAB HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Attachment B – Scope of Work

Contractor – CitizenLab

I. Awarded Scope / Executive Summary

The scope of this contract award includes the following category:

> Category 4 – Customer Engagement - A software solution that provides a centralized platform to manage multiple interactions with customers. Provides a platform for studying customer behavior through all channels and touchpoints of interaction such as phone, in-person, or online.

Additional Value Add Items / Services may be offered by Contractor within the Award Category listed above. Such value-added solutions may include, but are not limited to, solutions as - identity management, referrals engine, user behavior analytics, digital wallets, web hosting, Website & web app development, eCommerce services and payment processing, etc.

Executive Summary

CitizenLab is an online engagement platform that helps local governments convey information, collect feedback, and co-create programs and p[illegible]y with their communities. Over 500+ local governments around the world use CitizenLab to engage, consult, and deliberate with their residents and manage their ideas - both asynchronously and live through their one-of-a-kind online workshops feature. The platform's back-end project management tools help governments be more responsive and more efficient in their engagement efforts.

The company was founded in 2015 and has quickly expanded across Europe, and into the US. The US team is working with forward-thinking and innovative local governments, ranging from major cities like New York City, Wichita, and Seattle to smaller communities like Lancaster, PA. The company also has a research focus, and is seeking to build out expert partnerships, including projects with Ohio State University to host deliberative town halls with 20+ members of Congress.

The sections below include an overview of CitizenLab's core engagement features, value add items, and approach to blending technology with in-person support to help local governments shape and implement their own engagement strategy, and to make more informed and equitable decisions.

II. Core Features and Functionality

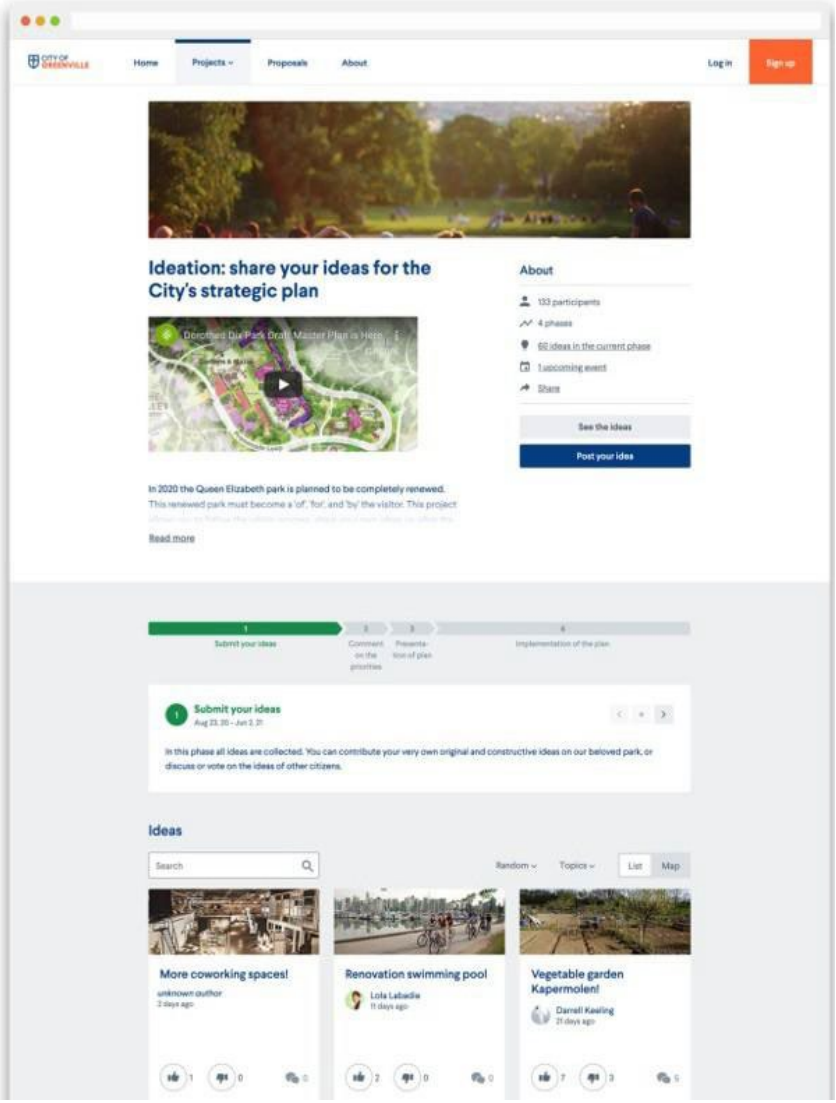
a. Introduction, Configuration and Overview

Ease of Use Functionality

This section will identify the various features available through the CitizenLab platform, with a focus on their ease of use, even for non-technical or not "tech-savvy" employees. The platform itself has two parts: a front-end and back-office, the latter of which is only available to Admins (and approved stakeholders). Both parts of the platform are backed by a series of onboarding and support services, as well as a series of support resources that can be accessed at any time by Admins (covered below).

Intuitive Design and Seamless User Experience

The CitizenLab platform provides a *simple and accessible user experience*, designed in collaboration with dozens of local government employees in the US and abroad. This intuitive experience is critical, as it allows the Admins to operate the platform with ease and confidence, and to do so efficiently without needing additional hires or adding dedicated FTE support.



Top: A project page for a new city park plan. Branding in top left corner, colors, font, and URL can all be c[redacted]mized to align with the St[redacted]online visual identity.

Middle: Project information (text, videos, attachments) easily uploaded by Admins. Below, green bars indicate project phases, which set expectations for residents on how and when to provide input (and how their input will be used).

Bottom: User generated ideas for their new park. Ideas and projects (and their data) can be linked to topics, locations, and user groups. Residents can upvote, downvote, and comment on other residents' ideas.

b. Platform Front-End: Configuration and Navigational Structure

Browser, Visual Identity, and URL: The platform is fully responsive, so it works with all major browsers and on computers, phones, and tablets. It is also white labeled, so it can match the State's existing identity via logos, colors, homepages, all to make the site feel local. States can also use a custom URL or host the platform as a subdomain on their website.
Pages / Home Page: The platform can act like a website in that it can provide one-way information, and feature images, videos, hyperlinks or attachments. The platform's Home Page provides the user with an overview of the active projects and folders. A folder can house several projects, often around a specific theme. The Home Page can be customized so that certain users can only see (or participate in) certain projects or folders.
Projects: A project represents a specific engagement initiative, and each project has its own dedicated page. There, users can learn about the project in detail, see relevant timelines and other participating users, and register for upcoming (in person or virtual) events. A project can have a set timeline or be continuous (without a timeline). The timeline shows the complete project broken down into phases from beginning to end. Each phase can have its own description, method of engagement, and start and end dates.
Ideas: Ideas are at the core of the platform, and allow residents and Admins to suggest, discuss, and vote on various recommendations and plans. Ideas are shown as "cards" with their title, image, author name, and the number of comments and votes (see above image). Users can filter the list of ideas by area or topic, or even search for specific content or keywords. Users can also sort ideas by date added, most popular (most votes), what's trending, or at random. This limits biases against early ideas receiving more attention. Every idea also has its own individual page, one that mirrors the structure of a project's page. Like a project page, users can read a description, see the idea's status, cast a vote, share it on social media, and interact with the author or other users. Admins can also provide official updates, which stand out from regular user-generated comments. *All ideas and projects can be organized by and linked to custom topics (e.g. climate, mobility, housing), location (e.g. neighborhoods), or user-groups (e.g. bus-riders).*
Sign-In: By default, a non-logged-in user (a participant) can view the platform, but not take action (e.g., vote, comment). Once signed in, a user's actions are tied to their account, so they will be unable to take the same action multiple times. Visitors can register with an email address (or phone number) and password or via their Facebook or Google accounts. User verification and forms of authentication are possible as well. During sign-in, Admins can request additional information (e.g. gender, city, age) from residents through custom registration fields, allowing for more granular insights. These fields can also link to group permissions (e.g., only residents from a certain city can vote on a project). Each user has a public profile page with all past ideas and comments made on the platform.

How does CitizenLab make this easy?

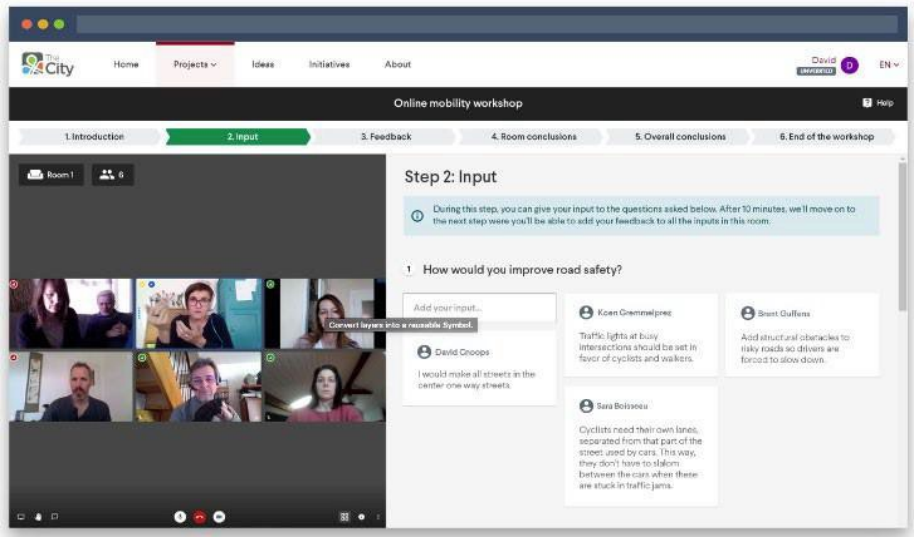
The onboarding and training support provided at the beginning of the contract cover all of the above features, including how to configure the platform and set up and design projects. Within one or two sessions, Admins will feel confident creating projects, defining idea requirements, and creating (and segmenting user data with) custom registration fields.

c. Platform Front End: Engagement Methods

Engagement Methods and Use Cases
Information: A project or phase can only provide information and is good for building context before or after asking residents to participate.
Surveys: CitizenLab has built-in survey tools, and can integrate with Qualtrics, Typeform, Google Forms, and other leading survey platforms. Surveys allow for a range of responses including short text, multiple choice, dropdown choice, etc. Surveys can also be designed with conditions and validation rules, and can include photos, icons, and videos.
Polling: Polls consist of one or more yes/no questions, (dis)agree statements, and multiple-choice questions. Polling data is usually anonymous, and online results can be combined with non-digital votes to increase engagement and inclusivity.
Option Analysis: Admins provide a set number of options, ideas, or scenarios on which residents vote and/or comment. This method allows Admins to start a discussion using a predetermined (and preapproved) set of choices. Here, residents cannot add their own options; they can only comment and vote in favor or against an option. For this and Ideation projects, users can also upvote comments, helping Admins to quickly identify the strongest/weakest arguments. Users can also directly address or involve other users and admins using the "@" sign. *This allows the platform to function as a space for residents to engage and debate ideas with one another.*
Q&A: Helps Admins gather quick, but open-ended answers that wouldn't fit into a poll.
Mapping: Great for planning and mobility projects, users pin ideas (or custom markers) on maps to collect ideas and feedback. Markers can represent multiple types of points of interest (e.g., restaurants, parks). Maps can feature custom layers to provide valuable context.
Ideation: Similar to an Option Analysis, except users submit their own options for others to debate and vote on. This approach is great for broad questions without a clear answer and for encouraging discussion between residents. *The screenshot above is an Ideation project.*
Participatory Budgeting (PB): Residents build their own budget by choosing from a predefined set of (admin or user-generated) ideas, each with their own price tag. While budgets and voting rules are set by Admins, PB gives residents insight and real power to shape State priorities.
Proposals: Proposals provide 'bottom-up' participation; allowing users to propose (and gather support for) their own initiatives, independent of Admin-created projects. Proposals range from simple requests, where users expect the State to take action (e.g., raise the driving age), to more open-ended requests based on broad needs (e.g., increasing road safety). *Proposals give residents agenda-setting power and act as a space for residents to weigh in on topics that may not be on Admin or State staff's radar.* However, like PB, Admins retain control over the structure, and many governments do use this feature initially or at all.

Asynchronous vs Live Engagement

CitizenLab's Online Workshops feature merges asynchronous and live community engagement. This custom-built, integrated tool enables Admins to run everything (registration, user data) through the platform, and includes closed captioning and recording functionalities.



Left: The left side of the workshop features video conference capabilities, while the right side allows for live polling, Q&A, breakout groups, and co-written input.

Governments around the world use this feature for virtual and blended meetings, town halls, and charrettes. Workshops can be linked to projects or specific user groups.

How does CitizenLab make this easy?

Successful engagement is more than correctly setting up a project on the platform. That's why CitizenLab's onboarding and continuous support is led by an engagement expert who also provides engagement strategy and communications frameworks, ideas, and best practices to ensure each project is effectively reaches and captures the right feedback from residents.

d. Platform Back-End (Back office): Feedback Management and Analysis Tools

The platform's back-office includes dozens of features and design choices to make managing and learning from engagement projects easy and intuitive. Rather than go into detail about each feature, the table highlights what these features *(in italics)* allow Admins to (easily) accomplish.

Build, Moderate, and Manage Projects: Using project *Templates*, Admins can set up a new project based on 26 proven formats (e.g. strategic plan, mobility plan, referendum), to save time and avoid "reinventing the wheel." For moderation, *Language Filters, User Flagging,* and *Bot Detection* tools help Admins keep user feedback on-topic and appropriate, and to prevent spam. These tools can be tied to a *Notification System* that CitizenLab helps set up based on the project content (i.e. is this a contentious issue?), State staff capacity, and communication preferences. This system also helps with content management. To reduce workload, Admins and Moderators can set up weekly *Automated Reports* that capture insights and activities in a given timeframe. To prevent duplicate ideas, our in-house *NLP tools* show users similar ideas already on the platform and invite them to post there instead.
Communicate with Users: Admins can drive residents to the platform via *Invitations* and bulk import email addresses. Once there, Admins and Project Moderators can respond to comments, change an *Idea Status*, and provide *Official Updates* on ideas using a clear name and role. These steps are visible to all users and are critical to making residents feel heard. Admins can also inform or update residents via

custom or automated *Newsletters* and can target users by region, *User Group* or user behavior on the platform. Like most popular email platforms, Admins can view campaign results within the platform (e.g. number of opens, clicks). *Social media sharing* is incentivized on the platform, and Admins and users can link and share ideas and projects on Facebook, Twitter, WhatsApp, and others. Users also have their own *Notification System* that keeps them informed on platform activities as they develop. States can also reach out to residents via built-in text/SMS tools that allow Admins to send text messages to residents with links to the platform, driving activity and participation from those that are less likely to be online or who don't have an email address.
Organize and focus on Specific Communities: A group is a collection of registered users on the platform. In a *Manual Group*, Admins manually select users for a group, often to bring existing groups (e.g., advisory panels) onto the platform. In a *Smart Group*, Admins can assign users to a group based on their demographic data or actions on the platform, and these groups grow with the platform. *Groups* allow Admins to focus on specific subsets of State residents by creating dedicated (i.e. private) projects or online spaces, creating custom emails based on user behavior or location, keeping residents updated on projects they care about, and analyzing and comparing data between different groups.
Collaborate and Coordinate Externally: The platform was designed to be used by multiple departments and organizations at once and facilitates collaboration. Admins can share *Templates* and *assign* specific projects, ideas, or comments to other Admins or Project Moderators, without providing access to the full platform. The platform also offers a *Widget* feature (requiring only a single line of HTML) that shows a customizable selection of ideas and a call to action to drive users to the platform and link existing State websites.
Analyze Feedback, Gain Insights, and Demonstrate Impact: The platform's *Dashboard* features shows all essential user and engagement metrics and can be filtered by time period, content (e.g. project, topic, user group), and mapped. All charts can be downloaded as PDFs and all data can be exported to Excel/CSV (or read via API) helping Admins manage and demonstrate platform impact. The platform's *Automated Reports* tool also pulls from these data and helps Admins compile reports or summaries for leadership, press, or the public. Using the platform's *Natural Language Processing (NLP)* technology, Admins can automatically organize open-ended text (e.g. ideas, comments) and cluster subsets of ideas based on content-similarity, which shows idea popularity within a topic or by demographic group and identifies keywords and larger trends. NLP saves Admins huge amounts of time reading through thousands of comments and helps them ask better questions in the future.
Get Help and Build Knowledge: Beyond the strategic support, CitizenLab provides support via a built-in chat system, phone hotline, and email on weekdays and Saturday except official U.S holidays. Admins will also have access to the *Knowledge Center,* an internal wiki with descriptions of every feature and answers to FAQs; *Guides and Resources,* written for government employees on a range of topics relevant to launching or running the platform; an *Organization Guide* which provides ideas on how Admins might organize internally; and *Partner Emails,* which provide tips, tricks, best practices, invitations to small group trainings, and updates on new features. In 2021, CitizenLab also rolled out a full Community of Practice for our hundreds of governments to encourage better sharing of best practices and ideas for those facing similar challenges.

A Note on Accessibility: The platform must be easy to use for all residents. CitizenLab complies with international standards on accessibility and is fully compliant with WCAG 2.1 AA guidelines. The platform is fully navigable by keyboard, images and buttons include 'alt-attribute' (so they work with screen readers), strong color contrasts to make text easier to read, and warns Admins should they make a decision that may impact accessibility.

III. Value Add Solutions

a. Value Add Items

The following items represent potential value-added options, features, and ideas that would benefit the work and push the field of citizen engagement forward. CitizenLab is already at work on some of these, and several items will be added to the platform in the coming months and years even without additional budgetary support from a State as part of this contract. However, should a State elect to include one of these items, these features can be prioritized and largely meet the timelines identified below. That said, all costs and timelines are estimates, and CitizenLab will work with a State to define appropriate timelines in advance of contract award.

VA #1: Sense-Making
Description: CitizenLab's current sense-making tools can scan and ingest all textual input generated on the platform, including hundreds or thousands of ideas, comments, and posts submitted by residents. The tool then provides Admins with insights by identifying keywords, themes, and basic sentiment by demographic details or location. Version 2.0 would allow for external Citizen-Generated Data (CDG) from external sources (e.g., social media, 311 services, other government-owned software) to be uploaded to the platform either as a simple CSV import or via API.
Value Added: Current sense-making allows Admins to ask broad, open-ended questions without having to manually read hundreds or thousands of responses. The sense-making tools do the initial analysis, providing Admins with easily understandable, pre-sorted feedback built around topics, projects, neighborhoods. This saves Admins hours, or even days worth, and removes the barriers that come with deeper and better engagement to take place on the platform. Version 2.0 would dramatically enrich this initial pre-sorted feedback, allowing Admins to analyze and compare the context-rich feedback made on the CitizenLab platform alongside multiple forms of external feedback (i.e. CDG) from a government's social media accounts, 311 system, chatbots, and other engagement tools. **The tool will also auto generate summaries of feedback on behalf of platform Admins.**
Documented Performance: CitizenLab is currently applying sense-making to auto generate project summaries, pulling from both qualitative and quantitative feedback submitted on the platform. These features have been successfully piloted with the Cities of Cincinnati, OH and Lancaster, PA, and the City of Seattle.
Cost/Schedule Impact: Once completely built, the tool will come included with the Premium Annual License. It is possible to expedite this process, but most likely not before Q1 2024. Development costs are directly tied to labor and would depend on timelines.

VA #2: Data Scraping + Public Data Dashboards
Description: As a first step towards realizing sense-making 2.0, CitizenLab would use data scraping techniques to pull data from a variety of existing engagement channels including, but not limited to: 311, social media, existing open (and cross-department) datasets, and then analyze these external data (i.e. CDG) against feedback on the CitizenLab platform. Instead of (or in addition to) integrating these data into the sense-making analysis (articulated in VA#1), data could also be hosted side by side with feedback from the CitizenLab platform on internal and public data dashboards.
Value Added: Having live data from these sources can often provide governments with a snapshot into resident sentiment and policy impact. *This feature would remove the need for many of the features currently included in Social Listening platforms (Category 5 of the RFP).* However, when compared with the deeper, more thorough feedback from the CitizenLab platform, Admins can uncover new insights and begin to understand the 'why' behind those initial snapshots. When used in tandem, Admins can also use one set of data to inform the other, creating an iterative, virtuous cycle in which governments can ask better questions of residents across all platforms.
Documented Performance: As mentioned above, CitizenLab is currently piloting this sense-making technology in Ohio and Pennsylvania, and has created several public-facing dashboards for the City of Seattle. The platform also has new Overview and Representative Dashboard features that pull from third-party tools like Google Analytics to capture visitor data, as well as from existing demographic datasets (e.g. US Census) to allow Admins to understand how well the collected feedback represents the broader community (e.g. 40% of feedback is from residents over 60, but those residents comprise only 20% of the population.)
Cost/Schedule Impact: Once built, the data scraping functionality will come standard with the Annual License. The Overview and Representative dashboards, as well as the pilots were included at no additional cost, and this offer can be extended to participating States. The data dashboard can be built in a matter of weeks and would cost approximately 10-15% of Year 1 costs, depending on timelines and needs.

b. Value Add Solutions That Involve Third-Party Software Solutions

Contractor must be the original software publisher of the solutions offered within its Awarded Scope. Contractor may nonetheless submit value added solutions that involve third-party software solutions. As Contractor chooses to offer third-party software solutions as part of its value-added offerings any third-party end user licensing agreements are included in this Master Agreement through Attachment E.

The third party end user license agreements will be at the discretion of each Participating State or Participating Entity to review, negotiate and/or utilize these documents within their Participating Addendum. Purchasing Entities that acquire third-party software solutions shall be subject to the end user licensing agreements distributed with such software, unless otherwise stated in a Participating Addendum or as negotiated between the Purchasing Entity and third-party software provider.

Third-Party Software Solutions: CitizenLab currently integrates with Konveio, a document engagement platform, as well as a handful of survey, communications, and engagement tools, including Typeform, Qualtrics, Survey Monkey, Google Forms, among others. We plan to expand this list via our new marketplace, which is slated for roll out by spring 2024. This marketplace will allow for dedicated integrations tied to text messaging, mapping tools, PDF annotation, and agenda scheduling, among

others.

IV. Service Approach.

This section covers the main components of the CitizenLab offering, along with a detailed approach to helping the States launch their own platform. There are three components to our work:

Platform Front-end	The "front page" for State residents, where all updates and projects are posted. This provides residents with a reliable online space to give feedback, and Admins with a central location to manage all participation projects. *The front-end makes engagement easy and intuitive, helping States to reach and hear from as many people as possible.*
Platform Back-office	This part of the platform is only visible to Admins and State staff. The back-office allows Admins to create new projects, monitor and manage feedback, conduct analyses of resident data to uncover insights and meet reporting requirements. The back-office is also where Admins and other State-level stakeholders (including those at City/County levels) can coordinate and collaborate on projects and engage specific subsets of State residents (e.g. residents over 50). *The back-office provides flexibility and allows Admins to operate autonomously and efficiently.*
Onboarding and Continuous Support Services	Technology only represents part of a successful engagement strategy. As such, CitizenLab will provide States with a dedicated engagement expert to serve as a Engagement Advisor (EA) throughout the contract. This person has run hundreds of online engagement projects at the local, regional, and national level, and can help guide Admins through the process. CitizenLab front-loads these services to ensure Admins can work comfortably and independently with the software. Once launched, the EA continues to provide strategy and analysis support, training on new features, and coordination with other State Departments as well as other governments where needed. In addition to the EA, CitizenLab provides access to a support team (technical and otherwise) and a library of resources, which will help Admins answer quick questions and make adjustments to the platform as needed.

Project Deliverables

The onboarding schedule below defines specific dates, but the key phases and deliverables to the CitizenLab offering include:

Phase	Deliverable
1: Kickoff / Onboarding	Outlined in detail in the table below, this phase is designed to help governments finalize their digital engagement strategy, learn the platform, let residents know about this new tool available, and build out the initial group of engagement projects. **Deliverable:** CitizenLab hosts Kickoff Meeting and Onboarding Meetings with key stakeholders from local government.
2: Platform Build and Launch	Also outlined below, this phase overlaps with Phase 1 and is dedicated to building and launching the platform for public participation. **Deliverable:** CitizenLab delivers a configurable platform to Admins and together launch they platform when ready.
3: Continuous Support	Outlined in a separate table, this phase begins once Phases 1 and 2 conclude, and coincides with the launch of the platform. During this phase, support is scaled back and focuses on strategic challenges that arise during the engagement process. **Deliverable:** Monthly meetings to ensure projects remain on schedule and goals are being met, and flexible ad-hoc meetings to address specific issues.

Onboarding and Platform Build Schedule (Phases 1 and 2)

The schedule below assumes a contract start date of June 1, 2021; all dates are estimates. The sessions below represent a baseline for onboarding services, and CitizenLab anticipates the process will be more fluid in practice (i.e. calls and messages with quick questions, etc.)

Milestone / Date	Description / Deliverable / Expectations
Project Kickoff *June 3 (90 min)*	Formalize core team (i.e. primary users/Admins) and introduce to EA. Participants will discuss platform primary uses and goals, community considerations, project timelines, as well as finalize tech requirements and formalize rest of onboarding schedule.
Platform Build *June 8*	Platform is configured to State specifications and ready to be populated by EA and State core team. See Attachment D.5 for details.
Participation Strategy Workshop *June 15 (60 min)*	EA helps the core team (and leadership) define the platform's role in larger participation strategy. Process is collaborative and helps Admins set goals and expectations for the upcoming contract year.
Comms Strategy Workshop *June 22 (60 min)*	EA works with core team (and relevant comms teams) to identify online and offline outreach strategies, with a focus on hard-to-reach constituencies. Focus is on raising awareness both broadly and within specific communities about platform's use and capabilities.
Training Session: Platform Build *June 29 (90 min)*	EA onboards core team on the platform's back-office (i.e. management tools), guides them through the set-up process and various platform features. Focus is on creating new projects.
Project Design Workshop *July 6 (90 min)*	EA helps the core team to scope and design participation projects, using e-participation canvas (see D4.2). Focus is to help think through project goals, wording, data collected, and other strategic considerations.
Platform Quality + Accessibility Review *July 13 (45 min)*	EA provides a thorough platform review, focusing on information quality and accessibility to ensure the platform is ready for public launch, meets accessibility standards, and is as inclusive and user-friendly as possible.
Training Session: Engagement / Use* *July 20 (60 min)*	EA leads a deep dive into best practices of the platform, with a focus on increasing resident adoption and use. Focus is on platform aesthetics, do's/don'ts, and other more granular features.
Final Review and Launch Meeting	EA conducts final review of the platform and works with the core team to finalize launch and immediate next steps post launch. Focus is on addressing any last-minute items or issues.

July 27 (60 min)	
Platform Launch *July 27*	Platform publicly launches in alignment with communications plan and residents begin providing feedback.

**As a 10th meeting, Admins can also set up a third training session for a broader group of stakeholders or on a topic of their choice.*

Continuous Support Schedule (Phase 3)

Meeting / Date	Description / Deliverable / Expectations
Check-In Meetings *Monthly (up to 10x)*	EA meets monthly with the core team to review progress, make adjustments where needed, and plan upcoming projects.
Flex Meetings *As needed (up to 5x)*	Potential uses include support for coordination between different departments or with local governments, preparation for large or potentially contentious projects, and data analysis support.

V. Service Assumptions

Assumptions made in this proposal fall into one of three categories: 1) how a State will use the platform; 2) Government and resident technical capacity and capabilities; and 3) A State's core team's staffing capacity to implement and manage the platform.

1: Assumptions of Platform Use / Goals

Online engagement is a relatively new development at the State level. Based on CitizenLab's work with regional, state, and national governments around the world, our team has made the following assumptions for how a State might use the platform once active. The table below articulates these uses, along with potential considerations and how CitizenLab can help maximize the effectiveness of each use.

Use Case	Description	Features
Statewide Referenda / Ballot Initiatives	Involve State residents earlier in the initiative selection process, ensuring initiatives have been openly discussed and reflect the will of State voters, not out-of-state companies.	*Proposal* and *Ideation* features let residents propose, choose, and discuss ideas in an open and transparent forum.
Feedback on Existing State Services	State residents can provide specific feedback on existing State-run services, including licensing and certification, and the criminal justice and education systems.	*Polls* and *Surveys* yield structured feedback; platform gives context on existing services, so feedback is informed.
Meetings / Public Comments	State residents can access past meeting agendas and notes, provide questions before/after meetings, and attend meetings via custom-built *Online Workshops* feature.	*Online Workshops* combine best-in-class video chat with live polls, Q&A, breakout rooms for small groups and town halls.
Strategic Initiatives	Raise awareness and get valuable early feedback on innovative projects like Broadband expansion. Long-term projects often benefit from open-ended resident ideas and feedback.	Using *Natural Language Processing*, even open-ended resident feedback can be analyzed to determine how well big initiatives meet their needs.
City, County, and State Coordination	Coordinate with city, county, and other state leadership and platforms (e.g. Gov2Go) to triage services and collaborate to better meet resident needs as they arise.	*API, Widget,* and *back-office* features allow for data-sharing, multi-site data collection, and delegation of responsibilities.

The CitizenLab team has made two additional assumptions:

1) Residents are often unsure about which level of government to turn to for a service; and

2) Many State-led initiatives may require input, buy-in, or support from city and county leaders.

As such, the CitizenLab team anticipates an increased level of coordination will be required and has enhanced *Ongoing Coordination Support* in the budget in Attachment C to reflect this need.

CitizenLab Assumptions of State Technical Capacity

CitizenLab assumes that a State government will have the technical capacity and systems to carry out this work. CitizenLab will need to work with someone from the State's IT department in order to launch the platform, and coordinate links to other websites, as well as launch the platform as a subdomain of the State website (or wherever the platform will be hosted).

While the platform has been designed with and for non-technical government employees, CitizenLab assumes the core team has a baseline level of experience working with Software-based platforms and are willing and ready to learn how to use the platform.

3: Assumptions of State Staff Capacity and Experience

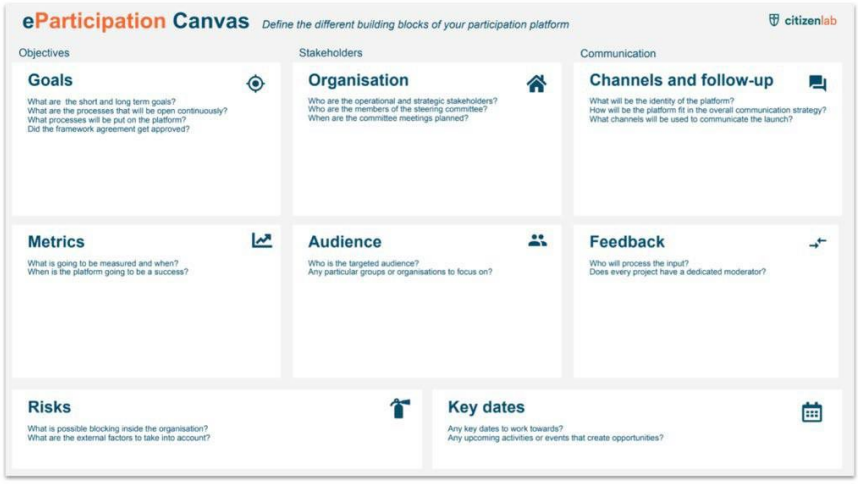
Buy-In/Experience: CitizenLab assumes that the State government staff, particularly the core team will have at least a baseline level of political, management, and cross-departmental buy-in, and has at least some experience or background in conducting in-person or online resident engagement. CitizenLab also assumes that by adopting the platform, State is making a long-term (i.e. multi-year) commitment to developing, managing, and growing an engagement strategy, and that this process does not necessarily yield success overnight.

Staff Capacity: CitizenLab assumes that staff have capacity (as measured in FTEs) to launch and manage various engagement projects. While there is no specific rule or number, CitizenLab recommends that at least **.25-.5 FTE be split up over 2 or 3 members of the core team** to implement this work during the contract period. This number will vary depending on the number of active projects, the type of projects, and the level of internal and external coordination required.

Multilingualism: CitizenLab integrates with WeGlot, a website translation tool that works in most major languages, translating all platform content at higher quality levels than Google Translate. This tool also improves over time, and can be paired with live translation services (e.g. Human-in-the-Loop) for near perfect translations.

The platform is also currently available in several languages, including among others English, French, German, Spanish, Danish, Dutch, Norwegian, Polish, Romanian, Portuguese and Arabic. Through a third-party integration, CitizenLab has enhanced translation capabilities that: 1) allow

residents who speak multiple languages to use the same platform; and 2) allow residents to converse with one another in their language of choice. However for CitizenLab's in-house feature, to limit miscommunication in all official materials, CitizenLab assumes that Utah government staff (not necessarily core team), have sufficient language capabilities to review all official attachments, videos, and project descriptions in English, Spanish, and any other languages to be featured on the platform. *Please note, this is not a necessity, but does help streamline translation processes. If this is not possible, CitizenLab recommends using the WeGlot integration, which does not require any in-house capacity to speak languages other than English.*



Left: *CitizenLab's e-participation canvas used during the engagement strategy portion of the onboarding process.*

CitizenLab assumes that Admins will have a baseline level of engagement experience and internal buy-in to lead this work.

VI. Roles, Responsibilities, & Exceptions

Live Platform Roles and Responsibilities

The Table in Section 5 - Service Assumptions breaks down the role of the CitizenLab EA during the initial onboarding process and after the platform's public launch. This section will focus on the variety of roles played by State government staff, including the core team, Admins, and other stakeholders within the platform, and how these roles work together to support the platform once launched.

Responsibilities: Advisory vs. Implementation

It should be noted that while the CitizenLab EA will play an active role in the design and development of the platform, the platform is designed to be run as autonomously and independently as possible by Admins. CitizenLab will play an advisory role throughout the contract, but it is the State team and Admins that will lead all implementation and execution of each engagement initiative.

Platform Roles

In order to maintain control over the data visible to different types of users, the platform employs a role-based system where users can be assigned to one or more roles. A role describes a function that a user exercises on the platform and determines their ability to perform actions and view content. The table below breaks down the roles and responsibilities of the State staff, as well as residents, and how these different users interact on the platform.

Role	Description and Responsibilities
Visitor *(Resident)*	Any visitor of the platform that does not register and log in is considered a visitor. By default, a visitor can see public projects and the corresponding ideas. Visitors cannot vote or comment without being logged in. To lower the threshold for visitors, they can initiate an idea, but will be asked to register right before they try to publish their idea - often referred to in design terminology as 'lazy log-in'.
User *(Resident)*	By default, users can interact - vote, discuss, and propose ideas - in all projects where they are granted access. Access can also be determined by a user's group affiliation (e.g. Salt Lake City resident) as a way to segment or focus on specific users and communities.
Verified User *(Resident)*	A user whose identity has been verified by the platform. This can be done via email and eventually text message confirmation and can be used to prevent spam accounts.
Project Moderator *(State Staff)*	Project Moderators oversee one or more specific projects. They can configure the design and manage the ideas shared (i.e. resident feedback) for any and all projects assigned to them. Project Moderators can also contact their project's participants and access project data on the platform's back-office dashboards. This role is crucial to allow for internal collaboration on the platform without creating dozens of admins and opening up access to all settings.
Platform Admin *(State Staff)*	Admin is the most powerful role on the platform and is only intended for staff members who need to manage the entire platform (e.g. State core staff). Admins can take all actions of previous roles. Additionally, they can change platform settings, manage all projects, groups, users, and assign Project Moderators.

Roles: Other Stakeholders

In addition to the roles identified within the platform, State government staff and other stakeholders will need to play additional support roles to ensure the platform runs smoothly. Specific roles will be determined during the Kickoff meeting, but some common roles include:

- *Politician / Management:* someone higher up in the management team or who can secure political buy-in;
- *Coordination:* someone who can play a coordination or administrative role, particularly as the number of stakeholders increases; and
- *Community Liaison:* someone who can coordinate with various community leaders on outreach and engagement as needed.

Each of these roles will play a critical part in ensuring that information is vetted and disseminated via the platform, that feedback is properly captured and analyzed, and that various departments within the State State government are able to collaborate effectively and efficiently.

State/Customer Technical Expectations of CitizenLab

The section below identifies several key technical responsibilities to be provided by CitizenLab. These steps are taken to ensure the platform runs smoothly for residents and State government staff, and that all visitors, users, Project Moderators, and Admins have an enjoyable experience.

Platform Hosting	The CitizenLab platform is a SaaS cloud solution and CitizenLab handles the initial technical implementation, maintenance, and any improvements made throughout the contract. Our team will set up all required server instances and databases. CitizenLab can also oversee DNS configuration and associated SSL configurations, unless State wishes to use its own domain. CitizenLab uses Amazon Web Services to host the application servers and databases.
Platform Uptime	The platform will be **available for more than 99.9% of the time**, measured monthly, with the exception of scheduled maintenance. Any downtime due to failure of third-party connections or utilities or other reasons beyond the control of CitizenLab will not be included in this calculation. Should the platform go down for an extended period of time, CitizenLab will compensate State based on the duration and frequency of the downtime. Downtime begins when State staff (or a resident) demonstrates that the server is down and continues until availability is restored.

Quality Control	In order to guarantee platform quality, CitizenLab: 1) regularly tests various software components including after changes to the code (e.g. releasing a new feature); 2) uses a runtime error tracking system that detects and aggregates errors as they occur, which helps our team understand the errors and the context in which they occurred, allowing our developers to easily reproduce and solve the problem; and 3) monitors memory usage, processor load, and general system load to detect and analyze suspicious usage patterns and alert the support team if an anomaly arises.
Performance	The software has been built redundantly to reduce risk and ensure a high level of availability. Servers auto-scale in order to stay afloat during peak times, allowing the platform to handle thousands of users at the same time without delay or issue.

VII. Risk Management Plan

The following items are potential risks that may emerge during an engagement initiative. While these risks all exist outside of CitizenLab's control, there are steps an Engagement Advisor, or platform Admins (and when needed the product team) can take to address and mitigate these risks for the future.

Risk #1 Low Platform Adoption
Description: Defined as lower-than-expected levels of engagement and participation on the platform, or users creating accounts, but rarely or never using them. This can happen for a variety of reasons often related to the circumstances in which the platform is launched. Low platform adoption can often be traced back to a mix of low public awareness, low existing levels of local trust, and poorly defined projects where community stakes are unclear.
Solution: CitizenLab provides robust onboarding support, including a range of upfront advisory, training, and outreach services during the first three to four weeks from contract launch. This work is almost entirely done prior to the public launch of the platform. This ensures that when a platform does launch, residents are aware of the platform and know how to access it, understand how their feedback will influence a decision, and believe that their feedback carries weight and will be heard. CitizenLab's on boarding support is led by a team of engagement experts. It incorporates best practices and strategies learned from our work with over 275 governments around the world and is designed to ensure the platform will be used by as many residents as possible. **Timelines/Cost:** This solution is included as part of our onboarding support costs and has been incorporated into the budget in Attachment C. The 3-4 week timeline is already built into CitizenLab's standard project planning.

Documented Performance: CitizenLab's work with The National Institute of Youth in Chile and in Lancaster, PA both reflect how these upfront services can drive engagement. In Chile, the platform hosts more than 40,000 users, and in Lancaster, the platform facilitated more than 13x the traditional feedback received from particularly hard to reach communities. Both governments have commended CitizenLab for driving engagement to their platforms.

Risk #2 Bad Behavior by Platform Users
Description: Defined as platform users (i.e. residents) engaging in uncivil discourse, using hateful or incendiary language, trolling, or any intentional behavior designed to disrupt the engagement and participatory processes hosted on the platform.
Solution: A combination of system- and human-led moderation. The CitizenLab platform includes automatic moderation features that prevent residents from using offensive or hateful language. Should residents make destructive comments without using foul language, comments can be flagged by other users and moderators can set up notifications that immediately alert them to offending comments, ideas, etc. For conversations that are anticipated to be contentious, Admins can implement settings that can give Project Moderators greater control over a conversation to ensure all voices are heard and the conversation remains productive. **Timelines/Cost:** These features are built into the Annual Platform License and thus carry no additional cost. While all platforms require some degree of moderation, this requirement is minimized as the flagging and notification system only alerts admins and moderators when issues arise. Based on historical experience this does not happen often.
Documented Performance: Current moderation features are built into all platforms and routinely help platform Admins and Project Moderators keep conversations civil and productive. CitizenLab will be rolling out an enhanced version (based on the same Natural Language Processing technology discussed in Attachment D.5), in June 2021 as part of a nationwide participatory program with the United Kingdom's Parliament, which due to its high-profile status, had increased requirements for content moderation.

Risk #3 Bot Accounts Altering Voting (Verification / Authentication)
Description: Defined as when a user acting in bad faith tries to manipulate vote counts or feedback metrics by either manually or automatically creating dummy accounts that cast votes in their favor.

Solution: When creating an account, CitizenLab can require users to verify their email and/or phone number. This extra step ensures one person to one account and has been proven to limit spam and bot accounts. As an additional precaution, the platform can also identify and alert Admins when multiple accounts have been created or used from the same IP address. When this happens, Admins can delete excess accounts and in certain situations ban a user entirely based on their IP address, preventing them from creating any new accounts.

While these solutions address user verification (i.e. they are a real person), they do not address user authentication (i.e. they are who they say they are). There are a handful of design choices that can be made to encourage only residents to sign up for the platform, but none are foolproof. In order to truly authenticate a user, users would need to provide additional identification information (e.g. driver's license number or SSN), which the platform can accommodate, but many local and regional governments in the U.S. opt to not include this feature.

Timelines/Cost: Current verification and some authentication features are built into all platforms and thus require no additional cost. Should a State be interested in enhanced authentication, there are a number of third-party integrations available, but these will depend on the level of authentication required. *As an estimate, costs would be under 10% of first year costs and would not disrupt the timelines if discussed in advance of contract start.*

Documented Performance: CitizenLab uses verification and authentication in a handful of European cities and towns where residents are asked to provide a national ID number in order to confirm their identity.

Deliverables

Table of Deliverables

Deliverable	Description	Due / Frequency
Platform Handover	CitizenLab will provide a configurable platform(s) ready for customization to State staff and platform Admins.	**10 days** after contract signature
Onboarding	An Engagement Advisor (EA) from the CitizenLab team will regularly meet with State staff and platform Admins in accordance with the onboarding schedule outlined in Section IV. EA will lead training, as well as strategic support on platform design, engagement methods, and communication best practices to ensure platform launch is successful and Admins are comfortable using all relevant platform features.	Onboarding Begins **10 days** after contract signature (unless otherwise specified by customer) and will be completed no more than **4 weeks** after process begins.
Platform Launch	The platform has been customized to align with State branding and existing digital assets, initial projects have been created with clear timelines, and is ready for public use and participation.	**60 days** after contract signature (unless otherwise specified by customer)
Regular Meetings + Check Ins	EA will meet regularly with Admins to check in on overall platform health, discuss specific projects, ensure goals are being met, and address strategic challenges that may emerge over time.	**Monthly**, or less as needed, with flexible ad-hoc meetings to address specific issues as needed.
Project Specific Data Reports	EA will coordinate with Admins and CitizenLab's in-house data team to generate project-specific reports on behalf of a customer. The purpose of these reports are to ensure Admins can easily report out and share on engagement and platform impact and that insights gained from engagement can be incorporated into State decision-making.	**1-4**, The format, number, and frequency of these will be determined prior to contract signature.

VIII. Financial Summary

CitizenLab Billing Structure and Payment Terms

All CitizenLab prices quoted are exclusive of Sales Tax, and any other taxes, costs, royalties, etc. CitizenLab typically invoices for all software provided (e.g. License Fee) and services rendered (e.g. Onboarding, Data Reports) with either a one-time invoice or, in the case of multi-year contracts, the Year 1 License Fee agreed upon in the Quote. For multi-year contracts, implementation fees, custom developments, and other services will be billed separately.

1.1 Payments shall be made in US Dollars, with no reductions applied due to taxes (e.g. sales tax), charges (e.g. bank charges), or any similar fees, whether fiscal or parafiscal, direct or indirect.

1.2 Any request by the Customer for additional developments by CitizenLab, shall be on mutually agreeable terms and conditions, including additional costs. Acceptance of the request by CitizenLab, as well as upfront approval from Customer on the development estimation, are required before any such developments shall be executed.

1.3 Where the Customer chooses another Pricing Plan midway through an active contract (i.e upgrade or downgrading their license), the following shall apply:

1.3.1 Upgrade from: Single Project to Standard or Premium, or Standard to Premium. The Customer shall receive an additional invoice for the prorated amount.

1.3.2 Downgrade from: Premium to Standard or Single Project, or Standard to Single Project. The Customer shall be entitled to prorated credit, which will be applied as a reduction on the next invoice or the Customer gets refunded for the credit amount within 30 days after the termination of the Agreement, if the contract is not renewed. The Customer shall pay all amounts due in accordance with the Agreement within thirty (30) days from the invoice date. If the Customer fails to make payment within the timeframe:

CitizenLab shall be entitled to late payment compensation of 8% of the amount due (minimum of USD $150), plus a conventional late payment interest on the overdue amount, equal to the product of (a) 9% on the due amount and (b) the number of days in which payment remains due, divided by 365.

CitizenLab shall be entitled to suspend the Services after ninety (90) days following the payment due date. CitizenLab shall notify the Customer of the suspension and shall only continue its obligations if the Customer provides sufficient security for the fulfillment of its payment obligations.

1.4 Late payment of an invoice causes all outstanding invoices of the Customer to become due, even if the due date of these invoices has not yet expired.

1.5 CitizenLab reserves the right, at the end of each Term of the Agreement, to formulate the renewal of the Agreement under the resolutive condition of acceptance by the Customer of modified terms and Fees. CitizenLab shall notify the Customer of a proposal for an amended Fee at least thirty (30) days prior to the Expiration Date of the current Term of the Agreement. The Customer shall notify CitizenLab in writing:

1.5.1 Agreeing to the modified terms and/or Fees no later than on the Expiration Date of the Agreement; OR

1.5.2 Disagreeing, which shall result in the termination of the Agreement after its Expiration Date.

IX. Contractor Contact List

CitizenLab Contact List

Personnel		**Role**	**Email / Phone**
Sarah Horton		Director of North America	sarah.horton@citizenlab.co
Finance		Billing and payments	billing@citizenlab.co
Stijn Zwarts (or another Support Specialist		Customer Support	stijn.zwarts@citizenlab.intercom-mail.co

Pricing

CitizenLab Premium license each year includes:

Seats

- 8 platform administrators
- Unlimited project managers

Features

- Custom styling options
- Custom platform structure
- ID verification & SSO
- Data insights module
- Custom platform URL
- Configurable homepage layout
- Configurable platform definitions
- Unlimited Project folders
- User segmentation and smart groups
- Online workshops module

Expert Services

- Design and accessibility review
- Premium onboarding (6 sessions)
- 2 expert sessions per year
- Priority client support

Year 1	**Recurring Year**	**5-Year Total**	**7-Year Total**
$279,000	$265,000	$1,339,000	$1,869,000

CitizenLab General Terms and Conditions

1. Definitions

1.1 In these General Terms and Conditions, the below capitalized terms have the following meaning:

- "Agreement": this Agreement consists of the accepted Offer, the General Terms and Conditions and its exhibits.

- "CitizenLab": CitizenLab Inc., having its registered office and principal place of business in the United States at 2093 Philadelphia Pike #1527, Claymont, DE 19703.
- "Customer": the (future) contracting party of CitizenLab with whom the Agreement is entered into.
- "Customer Data": any data that is generated through user input or uploaded by the Customer through the Services, as well as any data based on or derived thereof or provided to the Customer as part of the Services.
- "Confidential Information: all data that is non-public, business-related information, written or oral, whether or not it is marked as such, that is disclosed or made available to the receiving party, directly or indirectly, through any means of communication or observation. Confidential Information includes, but is not limited to, the terms of this Agreement, trade secrets, user data, and information not generally known to the public, such as business plans, strategies, practices, products, personnel and finance.
- "Disclosing Party" means the party that discloses Confidential Information to the Receiving Party under the Agreement.
- "Equipment": all devices and peripherals necessary to connect, access or otherwise make use of the Services, such as, but not limited to: modems, hardware, servers, software, operating systems networks, and web servers.
- "Expiration Date": the date on which the Agreement is terminated.
- "Fees": the amounts payable by the Customer for the use of the Services and for the implementation of the Services.
- "Force Majeure": any event or circumstance which is beyond the reasonable control and without the fault of the party affected, and which temporarily or permanently prevents the affected party from (further) performing its contractual obligations under the Agreement. Such events or circumstances are for example, without limitation: riots, wars, acts of terrorism; natural disasters; sabotages; strikes; epidemics of pandemics; interruptions and malfunctions of computer facilities;
- "General Terms and Conditions": these general terms and conditions, including its exhibits, which apply to every Offer made by CitizenLab, every acceptance by the Customer of an Offer, and in general to every agreement entered within that framework between CitizenLab and the Customer.
- "Intellectual Property Rights": all acquired and future intellectual property rights, including but not limited to copyrights, trademarks, design rights, patents, know-how, trade secrets, inventions, all applications for the protection or registration of these rights and all renewals and extensions existing in any part of the world and all other intellectual property rights protected by any applicable law.
- "License": the right of the Customer granted by CitizenLab to use the Services in accordance with the Agreement.
- "License Commencement Date": the date that the License commences, as detailed in the accepted Offer.
- "License Expiration": the date which the License expires, as determined in the accepted Offer.
- "License Fee": part of the Fee which is paid by the Customer for the use of the Services.
- "Maintenance Window": the time gap between 12 AM (midnight) and 6 AM EST from Mondays to Saturdays, and the entire day on Sundays and Official United States Holidays.
- "Offer": the explicit, written proposal from CitizenLab to the Customer to enter an agreement.
- "Partner": any party who has a contractual relationship with Citizenlab and who acts on behalf of CitizenLab with respect to one or more Services.

- “Pricing Plan”: the chosen set of Services (Single Project, Standard, or Premium).
- “Priority Support”: the level of support provided by CitizenLab to a Customer if the Customer opted in for a Premium Pricing Plan, of which the Service Level Objectives are detailed in Annex III.
- “Receiving Party" means the party receiving Confidential Information from the Disclosing Party under the Agreement.
- “Services": the services provided by CitizenLab to the Customer under this Agreement, including software (platform), know-how, as well as related improvements, extensions and modifications, that will be available and detailed in the applicable Pricing Plan.
- “Service Availability:” the time duration during which the Services are available, as measured in minutes over the course of a one-month period, hereby excluding minutes of a Maintenance Window and the minutes dedicated to emergency maintenance.
- "Service Credits": an amount to which the Customer is entitled if a Service Level Objective is not met by CitizenLab, of which the calculation and conditions are set forth in the Service Level Agreement.
- “Service Issues”: any interference of the Services as further detailed in the Service Level Agreement.
- "Service Level Agreement": the Annex III.A <OR> Annex III.B as attached to these General Terms and Conditions.
- "Service Level Objectives": the intended levels of the provision of the Services as described in the Service Level Agreement.
- “Support”: the support provided by CitizenLab to a Customer in the context of the Agreement, of which the Service Level Objectives are detailed in the Service Level Agreement.
- “Target Resolution Time”: under the condition that the Customer has opted in for a Premium Pricing Plan, the time gap between the notification of a Service Issue and the temporary or definitive resolution of the Service Issue. The Target Resolution Time is calculated within Working Days and is further specified in the Service Level Agreement.
- “Target Response Time”: under the condition that the Customer has opted in for a Premium Pricing Plan, the time gap between the notification of a Service Issue and the oral or written acknowledgement by CitizenLab of the Server Issue. The Target Response Time is calculated within Working Days and is further specified in the Service Level Agreement.
- “Term”: the current or renewed periods during which the Agreement is effective.
- “User”: any individual end user of the Services who is granted user access to the Services by the Customer.
- “Working Day”: Monday to Friday during the hours of 9:00 AM through 6:00 PM Eastern Standard Time (EST), with the exclusion of Official United States Holidays.

2. Conclusion of the Agreement

2.1 Every Offer is without obligation until acceptance by the Customer. With acceptance, an Agreement is deemed to have been fully and legally entered. The written or electronic signature of the Offer by both parties shall constitute such acceptance.

2.2 By entering this Agreement, it is assumed the Customer will accept these General Terms and Conditions and therefore waive the application of its own terms and conditions.

3. Delivery of the Services

3.1 CitizenLab shall make available the Services to the Customer from the License Commencement Date, in accordance with the Service Level Agreement and the other provisions of the Agreement. The Customer shall have the right to use the Services within the restrictions set out in the Agreement.

3.2 Subject to the terms hereof, CitizenLab shall provide the Customer with reasonable technical support services in accordance with the terms set forth in the Service Level Agreement.

3.3 CitizenLab has the right to deliver the implementation and/or general support aspect of the Services by its Partner(s).

3.4 The Customer may request CitizenLab to upgrade/downgrade their License to a different Pricing Plan. This can be done once per annum, per Customer. Such requests must be delivered by email to the Customer’s point of contact at CitizenLab. Such a change to a Pricing Plan

shall take effect upon acceptance by email by CitizenLab, which shall be no later than fourteen (14) days following the request of the Customer.

3.5 If CitizenLab is prevented by Force Majeure from performing or further performing the Agreement, regardless of whether the Force Majeure was foreseeable, CitizenLab shall be entitled, without any obligation to pay damages, to terminate the Agreement in whole or in part by means of a written notice without judicial intervention, without prejudice to CitizenLab's right to payment by the Customer for performance already performed by CitizenLab before there was a situation of Force Majeure or to suspend performance or further performance of the Agreement in whole or in part.

4. Service levels

4.1 CitizenLab commits itself by means of a best-effort obligation to provide the Services in accordance with the Service Level Objectives as determined in the Service Level Agreement.

4.2 If CitizenLab fails to meet the Service Level Objectives, the Customer is entitled to Service Credits, the calculation of which is included in the Service Level Agreement.

4.3 To the extent reasonably possible, CitizenLab will inform the Customer of any anticipated failure to meet a Service Level Objective and of the steps CitizenLab shall take (or has already taken), in order to avoid the failure to meet the Service Level Objective, in accordance with the Service Level Agreement.

5. Restrictions and responsibilities

5.1 The Customer commits that it shall not, to the extent permissible by mandatory law, when using the Services:

- Reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services or any software, documentation or data related to the Services.
- Modify, translate, create, or publish derivative works of the Services.
- Remove or obfuscate proprietary notices or labels of CitizenLab or third party proprietaries.
- Otherwise violate the Intellectual Property Rights of CitizenLab or third parties. The Customer also warrants and represents that it shall undertake commercially reasonable efforts to promptly remove from the Services any content uploaded by the Users that violates or may violate Intellectual Property Rights of any third party.
- Use the Services for time sharing or service bureau purposes or otherwise for the benefit of a third party.
- Upload malware, viruses, trojan horses, spyware or other similar malicious software.
- Upload and distribute illegal content and content that incites hatred, violence, discrimination or other illegal activities. The Customer also warrants and represents that it shall undertake its best efforts to promptly make available any content uploaded by the Users that violates or may the aforementioned cases.
- Use the Services for the purpose of distributing unsolicited electronic communications.
- Interfere, circumvent, or undertake any attempt thereof, with respect to the security features of the Services.
- Undertake any other act that may interfere with the functionality, availability, or integrity of the Services.
- Use the Services in any other way that violates other policies or instructions provided by CitizenLab. It shall be at the discretion of CitizenLab to implement or modify any policy or instruction.
- Use the Services in any other way that violates applicable regulations.

5.2 Furthermore, the Customer warrants and represents that it shall, while using the Services:

- Promptly obtain the consent of any owner of Intellectual Property Rights to use their works on the Services. If such consent is not obtained the Customer shall promptly remove or make unavailable such content without undue delay.
- Adopt secure IDs and passwords, and implement appropriate organizational measures with respect to passwords in relation to the access to the Services in line with any possible instructions provided by CitizenLab.
- Inform all Users of the Services (employees, officers, consultants) of these General Terms and Conditions.

5.3 If the Customer violates any of the above provisions. CitizenLab shall have the right to suspend the Customer's access to the Services, subject to a written notification by email, two (2) Working Days in advance. The Customer shall inform CitizenLab by email, of a potential solution. Upon acceptance by CitizenLab, the Customer shall use commercially reasonable efforts to remedy the violation within a reasonable time but no later than ten (10) Working Days. If the Customer does not remedy this violation, CitizenLab has the right (i) to remove the infringing content and (ii) to immediately terminate Customer's access to the Services and consider the Agreement as terminated in accordance with article 9, without prejudice to the right of CitizenLab to fully recover any damages from the Customer as provided under this Agreement

6. Confidentiality

6.1 The Receiving Party agrees not to disclose the Confidential Information to anyone other than the employees, affiliates and suppliers of the Receiving Party on a need-to-know basis, always provided that such employees, affiliates or suppliers are aware of the confidential or proprietary nature of the Confidential Information and are subject to confidentiality obligations equivalent to those set out in this Agreement.

6.2 The Receiving Party agrees: (i) to take reasonable precautions to protect such Confidential Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third party any such Confidential Information. The Disclosing Party agrees that the foregoing shall not apply with respect to any information after five (5) years following the termination of the Agreement or any information of which the Receiving Party can prove (a) it is generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Confidential Information of the Disclosing Party or (e) is required to be disclosed by law or pursuant to a court order.

7. Intellectual property

7.1 The parties acknowledge that all Intellectual Property Rights belonging to a party, prior to the execution of the Agreement, shall remain vested in that party, regardless of the execution of the Agreement.

7.2 The Customer shall own all Intellectual Property Rights on the Customer Data. CitizenLab shall own, or shall have the legitimate right of disposal, in all Intellectual Property Rights in connection to the Services. Nothing in this Agreement shall operate so as to transfer or assign any such Intellectual Property Rights to another party to the Agreement.

7.3 During the Term of this Agreement, the Customer is granted a non-exclusive, non-transferable, non-sublicensable License to use the Services subject to the Agreement and within the United States.

7.4 CitizenLab has the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, the Customer Data), and CitizenLab shall be entitled (during and after the Term hereof) to (i) use such information and the Customer Data to improve the Services and for other development, diagnostic and corrective purposes in connection with the Services and CitizenLab offerings, and (ii) disclose such information and the Customer Data solely in aggregated or other anonymized form in connection with its business. The Customer grants CitizenLab the right to create external communications and content for the purpose of amplifying and broadcasting the public project's on the Customer's platform. For any information that is not publicly available on the platform then consent must be granted by the Customer to CitizenLab, for the purposes in clauses 7.5.

8. Pricing and payment of Fees

8.1 All prices quoted are exclusive of Sales Tax, and any other taxes, costs, royalties, etc.

8.2 CitizenLab shall invoice the Services with a one-time invoice for the total amount, as agreed. Parties may derogate from one-time payment by agreeing to a yearly installment payment schedule, if the Term stretches over multiple years. Implementation fees, custom developments, and other services will be billed separately.

8.3 Payments shall be made in US Dollars, with no reductions applied due to taxes (e.g. sales tax), charges (e.g. bank charges), or any similar fees, whether fiscal or parafiscal, direct or indirect.

8.4 Any request by the Customer for additional developments by CitizenLab, shall be on mutually agreeable terms and conditions, including additional costs. Acceptance of the request by CitizenLab, as well as upfront approval from Customer on the development estimation, are required before any such developments shall be executed.

8.5 Where the Customer chooses another Pricing Plan in accordance with article 3.4, the following shall apply:

- Upgrade from:
    - Single Project to Standard or Premium, or
    - Standard to Premium

  The Customer shall receive an additional invoice for the prorated amount.

- Downgrade from:
    - Premium to Standard or Single Project, or
    - Standard to Single Project

  The Customer shall be entitled to prorated credit, which will be applied as a reduction on the next invoice or the Customer gets refunded for the credit amount within 30 days after the termination of the Agreement, if the contract is not renewed.

The Customer shall pay all amounts due in accordance with the Agreement within thirty (30) days from the invoice date. If the Customer fails to make payment within the timeframe:

- CitizenLab shall be entitled to late payment compensation of 8% of the amount due (minimum of USD $150), plus a conventional late payment interest on the overdue amount, equal to the product of (a) 9% on the due amount and (b) the number of days in which payment remains due, divided by 365.
- CitizenLab shall be entitled to suspend the Services after ninety (90) days following the payment due date. CitizenLab shall notify the Customer of the suspension and shall only continue its obligations if the Customer provides sufficient security for the fulfillment of its payment obligations.

8.6 Late payment of an invoice causes all outstanding invoices of the Customer to become due, even if the due date of these invoices has not yet expired.

8.7 CitizenLab reserves the right, at the end of each Term of the Agreement, to formulate the renewal of the Agreement under the resolutive condition of acceptance by the Customer of modified terms and Fees. CitizenLab shall notify the Customer of a proposal for an amended Fee at least thirty (30) days prior to the Expiration Date of the current Term of the Agreement. The Customer shall notify CitizenLab in writing:

- Agreeing to the modified terms and/or Fees no later than on the Expiration Date of the Agreement; OR
- Disagreeing, which shall result in the termination of the Agreement after its Expiration Date.

9. Term and termination

9.1 The Term is determined in the Offer. Either party can give notice, via email, if it wishes to terminate the Agreement upon its Expiration Date. This must be done thirty (30) days before the Expiration Date, and no later. If no notice is given, the Agreement will be automatically renewed for the same Term which commences the day after the Expiration Date.

9.2 The Customer acknowledges that the following circumstances shall by operation of law give rise to termination of the Agreement within the meaning of this article unless CitizenLab waives this termination in writing and pursues the performance of the Agreement to which CitizenLab is entitled:

- Insolvency of the Customer, such as bankruptcy.
- Any material breach of articles 5-7.
- Any other material breach of the provisions of the Agreement which the Customer fails to remedy within fifteen (15) days of being notified in writing of the breach by CitizenLab, such as, but not limited to, the non-payment of any pursuant to the Agreement within the agreed payment term. The aforementioned period of fifteen (15) days does not apply if the infringement by the Customer constitutes a criminal offense, or if the infringement compromises the functionality,

availability or integrity of the Services.

9.3 In the event of termination of the Agreement:

- CitizenLab shall make available all Customer Data to the Customer for electronic retrieval for a period of ninety (90) days. Thereafter CitizenLab shall retain the Customer Data only for three (3) months, after which CitizenLab shall either anonymize the Customer Data or remove it from all its systems. Such removal shall be confirmed in writing by CitizenLab upon request of the Customer.
- The Customer shall be encouraged and permitted to export, on an unrestricted basis, any and all user-generated data (incl. ideas, comments, proposals and user lists) via self-service means before the actual Expiration Date of the Agreement.
- Upon the Expiration Date of the Agreement, the Customer shall lose all administrator and moderation rights and shall have access revoked to the back-office of the Services.
- Subject to article 8.5 and to the Service Level Agreement, no refunds of the amounts paid shall be granted to the Customer.

9.4 All sections of this Agreement which by their nature should survive termination, shall survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

10. Warranty and liability

10.1 CitizenLab represents and warrants that:

- The Services shall be performed with reasonable skill and care in a timely and professional manner, using appropriately qualified and experienced personnel and in accordance with good industry practice.
- It shall use its reasonable efforts to ensure that the Services are free from all viruses and other contaminants including any codes or instruction that may be used to access, modify, delete or damage any data files, or other computer programs used by the Customer, and that for this purpose, CitizenLab warrants and represents that it shall use the most comprehensive and up to date available virus checker.
- This Agreement is executed by a duly authorized representative of CitizenLab.
- EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES CONTAINED IN ARTICLE 10.1, THE SERVICES ARE PROVIDED "AS-IS." CITIZENLAB 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. WITHOUT LIMITING THE FOREGOING, CITIZENLAB MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'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.

10.2 The Customer represents and warrants that:

- It owns or has obtained valid licenses of all Intellectual Property Rights in relation to the Customer Data uploaded on the Services.
- It owns a valid License for the Services with a clear mention of the License Commencement Date and License Expiration.
- It shall only use the Services in accordance with the terms of the Agreement.
- It shall not undertake any actions or participate in any conduct, even unrelated to the Services, which is intended, or could reasonably be expected, to harm CitizenLab, its reputation or its goodwill, or which could reasonably be expected to lead to unwanted or unfavorable publicity to CitizenLab.
- This Agreement is executed by a duly authorized representative of the Customer.

10.3 NOTWITHSTANDING ANYTHING TO THE CONTRARY, EXCEPT FOR BODILY INJURY TO A PERSON, IN NO EVENT SHALL EITHER PARTY, THEIR PARTNERS, SUPPLIERS, OFFICERS, AFFILIATES, REPRESENTATIVES, OR EMPLOYEES BE LIABLE TO THE OTHER PARTY FOR CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR ENHANCED DAMAGES, OR LOST PROFITS

OR REVENUES, ARISING OUT OF, RELATING TO, OR IN CONNECTION WITH ANY BREACH OF THIS AGREEMENT, REGARDLESS OF (A) WHETHER SUCH DAMAGES WERE FORESEEABLE, (B) WHETHER OR NOT CUSTOMER WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND (C) THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH THE CLAIM IS BASED.

10.4 EXCEPT FOR BODILY INJURY TO A PERSON, IN NO EVENT SHALL CITIZENLAB'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING OUT OF OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EXCEED THE LESSER OF: (1) THE TOTAL OF THE AMOUNTS PAID TO CITIZENLAB PURSUANT TO THIS AGREEMENT IN THE TWELVE MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE CLAIM; OR (2) THE AMOUNT FOR WHICH SUCH LIABILITY OF CITIZENLAB IS INSURED.

11. Indemnity

11.1 The Customer agrees to defend, indemnify and hold harmless CitizenLab, its officers, employees, agents, subsidiaries, affiliates and other partners, from and against any claims, actions or demands, liabilities and settlements including without limitation, reasonable legal and accounting fees, resulting from, or alleged to result from any conduct or misuse of the Services which infringes a provision of articles 5 to 7 (for example, the infringement of any Intellectual Property Right of a third party).

11.2 CitizenLab shall defend, indemnify and hold the Customer harmless from liability to third parties resulting from the infringement of any intellectual property by CitizenLab, provided upon discovery by the Customer, CitizenLab is promptly notified of any and all threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume primary control over defense and settlement. CitizenLab shall not be held to indemnification of the Customer for any settlement for which CitizenLab has not provided prior approval in writing.

11.3 The foregoing obligations do not apply with respect to portions or components of the Services:

- Not supplied by CitizenLab.
- Made in whole or in part in accordance with Customer's specifications.
- Modified after delivery by CitizenLab.
- Combined with other products, processes or materials where the alleged infringement relates to such a combination.
- Where the Customer continues to conduct infringing activities after being notified thereof or after being informed of modifications that would have avoided the alleged infringement.
- Where Customer's use of the Service is not strictly in accordance with this Agreement.

11.4 If, due to a claim of infringement, the Services are held by a court of competent jurisdiction to be or are believed by CitizenLab to be infringing, CitizenLab may, at its option and expense:

- replace or modify the Service to be non-infringing provided that such modification or replacement contains substantially similar features and functionality, or;
- obtain for Customer a license to continue using the Service, or;
- if neither of the foregoing is commercially workable, terminate this Agreement in accordance with article 9.

12. Miscellaneous

12.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.

12.2 This Agreement is not assignable, transferable or sublicensable by the Customer except with CitizenLab's prior written consent. CitizenLab may transfer and assign any of its rights and obligations under this Agreement without consent of the Customer. CitizenLab shall inform the Customer in writing in case of any such transfer or assignment.

12.3 This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications

and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein.

12.4 No agency, partnership, joint venture, or employment is created as a result of this Agreement and neither party has any authority of any kind to bind the other in any respect, except as specifically provided in this Agreement. In any action or proceeding to enforce rights under this Agreement, the prevailing party shall be entitled to recover costs and reasonable legal fees.

12.5 All notices under this Agreement shall be in writing or by e-mail and shall be deemed to have been duly given:

- When receipt is electronically confirmed, if transmitted by facsimile or e-mail.
- The day after it is sent by post letter.
- The date of confirmation of receipt, if sent by certified or registered mail.

12.6 This Agreement and all related documents, and all matters arising out of or relating to this Agreement, whether sounding in contract, tort, or statute are governed by, construed in accordance with, and enforced under the laws of the State of Delaware, without giving effect to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the laws of any jurisdiction other than those of the State of Delaware. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

Annex III.A: Service Level Agreement (Essential and Standard)

1. Service Level Objectives

1.1. This Service Level Agreement shall provide the Service Level Objective. To the extent there are any inconsistencies, the provisions of the Service Level Agreement shall prevail over the General Terms and Conditions. However, any conflicting terms in the accepted Offer shall prevail above the Service Level Agreement.

1.2. CitizenLab shall, during the Term of the Agreement, ensure the Service Level Objective of a Service Availability of 99.9%, measured monthly. Downtime shall begin to accrue as soon as the Customer gives written notice to CitizenLab that downtime is taking place, accompanied by any sort of evidence of the downtime, and continues until the availability of the Services is restored.

1.3. In the event where CitizenLab fails to meet the Service Level Objective, Customer shall be entitled, upon its written request, to the following Service Credits, which shall be compensated on the first month following such event:

- Service Availability <99%: reimbursement of 10% of the License Fee, prorated over a one-month period in the first full month following such failure.
- Service Availability <99.5%: reimbursement of 5% of the License Fee, prorated over a one-month period in the first full month following such failure.
- Service Availability <99.9%: reimbursement of 1% of the License Fee, prorated over a one-month period in the first full month following such failure.

1.4. If and insofar the Service Level was not reached due to Force Majeure, the previous paragraph shall not apply.

1.5. The cumulative amount of Service Credits for a one-month period, shall not exceed the total Fee prorated over a one-month period, nor the amount for which CitizenLab's liability has been insured.

1.6. The Service Credits shall be applied to the portion of the Fee that was paid in the month in which the Service Level Objective was not met.

2. Support hours and contact information

2.1. CitizenLab shall provide Support to the Customer per email (support@citizenlab.co) or by responding to helpdesk tickets via the CitizenLab platform on Working Days.

Annex III.B: Service Level Agreement (Premium)

1. Service Level Objectives

1.1. This Service Level Agreement shall provide the Service Level Objective. To the extent there are any inconsistencies, the provisions of the Service Level Agreement shall prevail over the General Terms and Conditions. However, any conflicting terms in the accepted Offer shall prevail above the Service Level Agreement.

1.2. CitizenLab shall, during the Term of the Agreement, ensure the following Service Level Objectives:

1.2.1. CitizenLab shall, during the Term of the Agreement, ensure the Service Level Objective of a Service Availability of 99.9%, measured monthly. Downtime shall begin to accrue as soon as the Customer gives written notice to CitizenLab that downtime is taking place, accompanied by any sort of evidence of the downtime, and continues until the availability of the Services is restored.

1.2.2. CitizenLab shall handle Service Issues via the following Priority Support Services:

Definitions of Priority Levels	
Priority Level	Description
Critical (Level 1)	The Services, or a critical function, is not functioning properly or integrally unavailable, causing significant impact to the Customer's operations. Errors that cause data to be lost. No work-around acceptable to the Customer is available. Examples could include: - Availability of Workshops or one of its critical functions; - Critical project (folder) functionalities for live projects; - Loss of critical data, such as registration and project data; - Systemic login, invitation, or registration issues (encountered by +10% of all users).
Major (Level 2)	One or more non-critical functionalities of the Services are unavailable or present major issues, causing significant impact to the Customer's operations. An acceptable and temporary work-around is available to the Customer. Examples could include: - Inability to save changes to a project (folder), or edit pages; - Inability to perform data exports; - Email campaign does not send out; - Inability to add new input by admins or users; - Severe loading speed issues (>5s loading time); - Problems with entering feedback and updating statuses.
Minor (Level 3)	The Services are available, but one or more of its functionalities present issues that have little to no impact on the work of the Customer. Operations could be improved by correction of a minor error. Examples could include:

	- Problems embedding a survey; - Support service task requests; - Other unusual invitations, login, and registration issues.
Minimal (Level 4)	The Customer requires information or assistance about the Services, such as questions about capabilities, installation, configuration, operation, cosmetic, … Examples could include: - Setting up user verification; - Changes to privacy policy, terms and conditions, etc.; - Adding custom registration data; - Product feedback and feature requests; - Changing color, header, logo, image, copy, language settings.

Error Response and Resolution Commitments		
Priority Level	Target Response Time	Target Resolution Time
Level 1	9 hours	2 Business Days
Level 2	1 Business Day	4 Business Days
Level 3	2 Business Days	10 Business Days or next software release
Level 4	5 Business Days	Undefined

The Targeted Response Time shall be measured from the moment the Customer gives the written notice until the moment the CitizenLab support team acknowledges receipt of the notice. CitizenLab shall provide Support as outlined in this section set forth for specific priority levels in the table above.

I.3. In the event where CitizenLab fails to meet a Service Level Objective, Customer shall be entitled, upon its written request, to the following Service Credits, which shall be compensated on the first month following such event:

- Service Availability <99%: reimbursement of 10% of the License Fee, prorated over a one-month period.
- Service Availability <99.5%: reimbursement of 5% of the License Fee, prorated over a one-month period.
- Service Availability <99.9%: reimbursement of 1% of the License Fee, prorated over a one-month period.
- Failure to meet a Targeted Response Time or a Targeted Resolution Time in the context of a Critical Service Issue: reimbursement of 10% of the Fee, prorated over a one-month period.
- Failure to meet a Targeted Response Time or a Targeted Resolution Time in the context of a Major Service Issue: reimbursement of 5% of the Fee, prorated over a one-month period.
- Failure to meet a Targeted Response Time or a Targeted Resolution Time in the context of a Minor Service Issue: reimbursement of 1% of the Fee, prorated over a one-month period.

1.4. If and insofar one or more Service Levels were not reached due to Force Majeure, the previous paragraph shall not apply.

1.5. The cumulative amount of Service Credits for a one-month period, shall not exceed the total Fee prorated over a one-week period, nor the amount for which CitizenLab's liability has been insured.

1.6. The Service Credits shall be applied to the portion of the Fee that was paid in the month wherein the Service Level Objective was not met.

2. Support hours and contact information

2.1. CitizenLab shall provide Priority Support to the Customer via telephone (via one of the phone numbers listed on CitizenLab's website), per email (support@citizenlab.co), or by responding to helpdesk tickets via the CitizenLab platform on Working Days.

-- END OF ATTACHMENT B --