CONNECTICUT HEALTH INSURANCE EXCHANGE
d/b/a ACCESS HEALTH CT

REQUEST FOR PROPOSALS (RFP)

FOR

HEALTH INSURANCE EXCHANGE

INTEGRATED ELIGIBILITY AND ENROLLMENT

PLATFORM

SEPTEMBER 23, 2025

TABLE OF CONTENTS

APPENDICES:

APPENDIX A – HIX PLATFORM MODERNIZATION

APPENDIX B – REQUIREMENTS TRACEABILITY MATRIX

APPENDIX C – INDEPENDENT CONTRACTOR AGREEMENT

APPENDIX D – Ethics Form 1 – GIFT AND CAMPAIGN CONTRIBUTION CERTIFICATION

1. BACKGROUND

The primary mission of the Connecticut Health Insurance Exchange d/b/a Access Health CT ("Access Health," the "Exchange," or "AHCT," or "we," "our," "us," or their capitalized counterparts), Connecticut's official state-based health insurance marketplace, is to decrease the number of uninsured residents, improve the quality of healthcare, and reduce health disparities through an innovative, competitive marketplace that empowers consumers to choose the health coverage that gives them the best value.

Our Values in Action

At Access Health CT, it is with our customers and our employees in mind that we seek to promote these collective values and to live by these behaviors. Our culture of acceptance welcomes and values everyone. We challenge the status quo to find new ways to grow and improve our community, our company and ourselves. Our people take pride in the service we provide, and in the spirit of the common good that we share.

- **Authenticity**: Act with sincerity, credibility and self-awareness
- **Integrity**: Commit to doing the right thing with genuine intention
- **Excellence**: Aim high and challenge the status quo
- **Ownership:** Take responsibility and initiative
- **One Team**: Collaborate to succeed
- **Passion**: Dedication to creating opportunities for great health and well-being

2. SCOPE OF WORK

The selected Respondent must enter a contract with the Exchange, substantially in the form of the draft contract set forth in **Appendix C** (the "Contract").

The Exchange encourages minority, women-owned and disadvantaged businesses to apply.

1. Overview of Current Platform

AHCT is Connecticut's official state-based health insurance marketplace, established in 2011 by Connecticut Public Act 11-53 to meet the requirements of the Patient Protection and Affordable Care Act (the "ACA"). AHCT's marketplace allows Connecticut residents to shop, compare, and enroll in quality health and dental plans, and it is the only place where residents can qualify for financial help to lower their costs, and if eligible, enroll in low or no-cost coverage through HUSKY Health (Medicaid and the Children's Health Insurance Program ("CHIP")) or the Covered CT Program, a program that offers no-cost health and dental insurance and non-emergency medical transportation to eligible Connecticut residents.

AHCT, in partnership with the Connecticut Department of Social Services ("DSS"), Connecticut's state Medicaid agency, operates an integrated, online eligibility and enrollment system (known as the Health Insurance Exchange (HIX) platform (the "HIX Platform")), that supports a single enrollment application used to determine applicants' eligibility for health and dental plans, financial help, and low and no-cost coverage through HUSKY Health or the Covered CT Program. The HIX Platform provides a seamless and real-time eligibility and enrollment experience. AHCT is the only place where Connecticut residents may qualify for financial help to help lower the costs of Qualified Health Plans ("QHPs"). Specifically, residents may qualify for Advanced Premium Tax Credits ("APTCs"), lowering monthly QHP premiums, and Cost-Sharing Reductions ("CSRs"), lowering the amounts QHP enrollees pay out-of-pocket for deductibles, co-insurance, and co-payments when receiving medical care.

Connecticut residents are able to access the HIX Platform from any device—laptop, PC, mobile phone, tablet, etc.—to complete their application for health and/or dental coverage, provide documentation to verify attested information, report changes to their household demographics and/or income, and terminate or renew coverage. If needed, applicants and enrollees can obtain free help with any of these processes by reaching out to AHCT's call center by phone or live chat, by contacting a Navigator, a Certified Broker or a Certified Application Counselor, or by attending an in-person enrollment event. Information provided on the application is verified via trusted electronic data sources whenever possible. However, there are instances where an applicant may need to provide additional information to complete an initial enrollment or renewal.

Starting in 2026, the annual Open Enrollment ("OE") Period will begin on November 1 and end no later than December 31. During this time, individuals and families are able to enroll in or renew a QHP and/or Stand-Alone Dental Plan ("SADP") for the upcoming plan year. Enrollments completed during this time will be effective January 1. Outside of the OE Period, most individuals must experience a Qualifying Life Event ("QLE") to be eligible to enroll in QHP and/or SADP coverage.

Medicaid/CHIP programs do not follow the OE cycle, and, therefore, individuals who are eligible for these programs can enroll at any time of the year. In addition, individuals who are American Indians or Alaska Natives, or who qualify for the Covered CT Program, can enroll in coverage at any time of the year. Individuals within a single household, and therefore on the same application, may be eligible for and enroll in different types of health or dental coverage.

AHCT electronically transmits all enrollment information to the applicable commercial insurance carrier(s) or DSS for processing. All communications regarding payments or benefits are shared by the carriers or DSS; therefore, AHCT will direct any questions regarding benefits or billing accordingly.

All individuals and families who complete applications may choose to receive standard notices from AHCT electronically (delivered to their secure AHCT online account) and/or via USPS standard mail. If an applicant provides a cell phone number to AHCT, then they are also able to consent to receiving information via text messages from AHCT and/or DSS. AHCT will also issue Form 1095-A to all individuals and families who were enrolled in a QHP at any point during a tax year, and those individuals and families who received financial assistance for their monthly premium in the form of APTCs will need Form 1095-A to reconcile their APTCs when they file their federal income tax return for such tax year.

The HIX Platform utilizes role-based access to ensure a worker using the system only has visibility to authorized information. General types of users are primary applicants, staff, third-party workers, and brokers. However, the system is configurable to add other types of users when necessary.

2. Overview of New Platform & Implementation Services

The Exchange seeks a qualified Respondent to design, develop, and deploy a new HIX Platform (hereinafter, the "New Platform" or the "Solution"), in accordance with the following:

a. The New Platform must be a secure, simple, user-centric platform which must adhere to all existing standards and requirements, while being scalable and capable of accommodating future changes. The New Platform must be designed in a user-centric manner, making the application process and language as simple and intuitive as possible. The New Platform must be architected using best practices and technologies which allow for rapid deployment of new and/or changed features and requirements, as well as modular integration with other tools, as warranted. The New Platform must leverage data from trusted sources, whenever possible, and incorporate Artificial Intelligence tools to improve the efficiency of the workflow and overall user experience.
    i. The New Platform requirements can be found in the Requirements Traceability Matrix (the "RTM"), attached to this RFP as **Appendix B**.
    ii. The New Platform must comply with all data integration requirements, as mandated by the Centers for Medicare & Medicaid Services ("CMS") and the Internal Revenue Service ("IRS"), for connectivity to the Federal Data Services Hub ("FDSH") and any other data sources identified by AHCT or DSS.

iii. The selected Respondent must retain resources/personnel who are knowledgeable and experienced in User Interface/User Experience (UI/UX) design.
iv. The New Platform must integrate with existing platforms for group health coverage, including the Exchange's Small Business Health Options Program ("SHOP") platform, and the Exchange's BusinessPlus platform, which among other things, allows employers to offer and administer Individual Coverage Health Reimbursement Arrangements ("ICHRAs").

b. Marketplace Production Environment
   i. By the Platform Operation Readiness deadline, which is set as June 2027, the selected Respondent must configure, and release a public-facing marketplace production environment, that meets all requirements in accordance with contracted terms and conditions.
   ii. The marketplace production environment must contain the data from the Data Conversion and Migration Plan.
   iii. The selected Respondent must guarantee the continuous and current availability and functionality of the New Platform and allow users access to the New Platform in advance of the 2027 Open Enrollment Period for Plan Year 2028, meeting the standards set by the Platform Operation Readiness guidelines. Users with coverage spanning Plan Year 2027 must also be able to use the New Platform to report household demographic and income changes, etc.
   iv. The selected Respondent must include and make available all QHP and SADP data from the staging environment, in the New Platform to allow applicants to compare options anonymously and shop throughout a plan year.

c. New Platform Deliverables
   i. AHCT requires the selected Respondent's New Platform implementation services to include the following deliverables:
      1. Functional Design Document: This document must comprehensively detail the functional design of the selected Respondent's proposed New Platform, including details regarding the proposed New Platform's security functionality.
      2. Interface Documentation: The selected Respondent must deliver documents that include all real time and batch interfaces comprehensively. The selected Respondent must also provide any recommendations for future enhancements.
      3. Technical Design Documentation: The selected Respondent must deliver comprehensive and complete technical design documentation for the proposed New Platform, detailing overall system architecture, database design, technologies and tools to be used, integration with other internal and external systems, as well as security and performance considerations. The selected Respondent must describe the processing and functionality of the following topics:
         a. Interface relationships, dependencies, and formats;
         b. Interface design elements, assumptions, and constraints;
         c. Transactional, data validation, and business rules;

    d. Event and error handling;
    e. General processing steps;
    f. Data mapping and transformation; and
    g. Privacy, security, and performance
4. Data Dictionary: The selected Respondent must deliver a data dictionary, database schema diagram, and an entity-relationship diagram with specifics related to elements that will be necessary for related data conversion. Data conversion must also be completed by the selected Respondent.
5. Implementation Plan: The selected Respondent must deliver an implementation plan to organize and roll out the project implementation activities to allow for the transition to Maintenance and Operations activities. This plan must specifically support AHCT and DSS through the aforementioned processes, while also outlining the specific roles related to the selected Respondent and AHCT/DSS respectively.
    a. The selected Respondent must provide a work plan detailing the estimated timeline for the implementation process.
6. New Platform Status Reports: Prior to Final State Deadline, the selected Respondent must deliver weekly updates on the status of the proposed New Platform. A status report must include, at minimum, an overall project status update, updates related to the status of functional areas, as specified by AHCT, and any schedule/deadline related updates. These reports should also include any information that the selected Respondent would like to alert AHCT of, related to, but not limited to, concerns, risks, obstacles, issues, resource constraints, and/or other specifics that may impact the project and/or project timeline. At the point of operational readiness of the New Platform, the selected Respondent must deliver a status report to AHCT. AHCT reserves the right to modify the frequency of the delivery of status reports.
7. Requirements Document: The selected Respondent shall allow revisions of requirements throughout the construction and performance testing period. Prior to final state deadline, the selected Respondent must provide any and all documentation related to testing results proving that the proposed New Platform meets all requirements set forth in the parties' requirements document. The selected Respondent must keep the requirements document up to date in a comprehensive manner including all requirements from the initiation phase, construction phase, and any/all change orders/requests. The requirements document must also be updated to reflect the state of the New Platform throughout the project and changes. suggested/performed during operations and maintenance.
8. Gap Analysis Documentation: Using information derived from the requirement elaboration and specification meetings, the selected Respondent shall develop and distribute a document detailing any and all gaps found between the requirements document and the proposed New Platform. The selected Respondent is also responsible for detailing

proposed solutions to the aforementioned gaps. It is expected that the gaps discovery process will begin upon the start of the implementation of the proposed New Platform.

9. Regulatory Cooperation and Documentation: The selected Respondent is required to provide expert and content-based input to AHCT, DSS, and any other entities, as requested and/or required.
10. Cooperation with Project Management, Independent Quality Management Services, and Enterprise Information Services: The selected Respondent is required to cooperate with the project management, quality management, and enterprise information teams, and any other internal or external stakeholders, as requested by AHCT. The selected Respondent is required to meet all standards set by the aforementioned teams and stakeholders, as well as any and all requirements set by other oversight teams (set by AHCT and DSS). The selected Respondent must adhere to all applicable industry best practices.
11. Turnover Plan: The selected Respondent is required to deliver a detailed and complete description of the proposed method to allow for turnover planning in the event the contract between AHCT and the selected Respondent is terminated, including information regarding, but not limited to the following:
    a. A summary of the support the selected Respondent will provide for any/all turnover activities;
    b. Identification and submission of all documentation, records, and other forms of data required for AHCT/DSS and its related entities to continue the design, development and implementation of the New Platform;
    c. Any and all resources and/or training materials that AHCT/DSS and related entities require or request to be able to complete the design, development, and implementation of the New Platform;
    d. Suggestions for reporting, tracking, and/or documenting any turnover results; and
    e. Documentation and verification of secure and precise transfer of data to maintain and ensure data confidentiality, accessibility, and integrity.
12. The selected Respondent must ensure that all deliverables appropriately and comprehensively meet project management best practices and standards.
13. A Plain Language Guide, such as what is found on https://www.plainlanguage.gov/.
14. The selected Respondent must conduct and provide the results of security scans at code and infrastructure levels.

d. Required Activities
    i. Deliverables, documentation, and related information must be shared with authorized organizations, official contacts, and/or any entities involved in the

federal or state review of the proposed New Platform. The selected Respondent must address any questions, concerns, and/or related suggestions, as set forth by AHCT/DSS and its related entities, as well as DSS. AHCT reserves the right to request periodic changes and/or refreshes during the testing/performance period through the final state deadline.

ii. Requirement Elaboration and Specification Meetings: The selected Respondent is responsible for organizing any and all activities related to, but not limited to, programming and design sessions with AHCT/DSS or related entities, as requested by AHCT or DSS. The selected Respondent is responsible for organizing meetings with appropriate stakeholders to allow for a complete and thorough understanding of current and anticipated user requirements, workflows, and existing and anticipated user priorities. The selected Respondent is also responsible for a complete and thorough understanding of current state processes to create a satisfactory future state product.

e. Proposed Timeline

i. A Respondent must meet the following key dates:

Event	**Deadline**
Execution of Contract	No later than April 2026
Development Start Date	No later than May 2026
Solution Go-Live Date	June 2027

3. Maintenance and Operations Services

In addition to the aforementioned implementation services and deliverables, the selected Respondent must provide the following ongoing Maintenance & Operations ("M&O") services upon successful deployment of the New Platform:

a. The selected Respondent must provide ongoing M&O services to the Exchange. The selected Respondent must supply the necessary staffing and support to ensure all M&O services are provided to allow for the ongoing functionality, accessibility, and operation of the New Platform.
b. The selected Respondent must provide services during normal AHCT business hours; however after-hours, on-call support may be required, as needed, to support certain activities.
c. In general, the selected Respondent must ensure ongoing functionality and availability of the marketplace production, training and testing environments, collaborating with AHCT and other vendor resources, as required.
d. The selected Respondent must provide the following services:
    1. System Maintenance: Activities outlined in the AHCT Maintenance and Operations Manual which remove and/or repair processing or performance errors, prevent system errors or vulnerabilities, and ensure compatibility with new technology standards or new software/operating system releases.

2. System Availability Management: Activities related to the monitoring, reporting, and optimization of the supported systems, including, but not limited to, resource usage, performance degradation or issues, task automation recommendations, and delivery of root cause analysis (RCA), as applicable.
3. Batch Management: Activities related to scheduling, executing and monitoring batch processes across supported environments, including remediation of batch failures and issues.
4. Incident Management & Resolution: Activities outlined in the AHCT Incident Management Manual related to management, review, triage, analysis, and disposition of incidents reported in production, training and testing environments.
    a. Data Corrections: Activities related to the development and execution of ad hoc or recurring scripts to address data issues resulting in loss of system functionality or block use of benefits.
    b. Platform Code Fix: Activities related to the design, development, test and deployment of critical priority incidents, when required by AHCT.
    c. Coordination and Communication: Activities related to communication with resources from AHCT and/or other vendors, as needed, to discuss, analyze, resolve and prevent future instances of production incidents.
5. Configuration & Deployment Management: Activities, as outlined in the AHCT Maintenance & Operations Manual, related to the configuration and deployment of software builds/releases, including, but not limited to, server and environment management, user profile management, version control, maintenance of source code repositories, etc.
6. Disaster Recovery & Support: Activities related to preparing, maintaining and testing Disaster Recovery plans for the New Platform.
7. Security: Activities related to the scanning, monitoring, reporting and resolution of incidents involving access, user credentials, network security, etc.
8. Consistent and ongoing compliance with responsibilities, as specified by AHCT.
9. Maintenance and updates to the New Platform, as required, including, but not limited, to any requested modifications or updates required by AHCT.
10. Assured compliance with any and all change management processes, as specified by AHCT.
11. All changes impacting the New Platform must adhere to the Hybrid Agile methodology, as specified in the AHCT Maintenance and Operations Manual, which includes a comprehensive release testing plan, application and security scans, and performance/load testing (to be performed by the selected Respondent) prior to each major release and on an ad hoc basis, as requested by AHCT.

12. All documentation/manuals must comply and align with most up-to-date New Platform functionality.
13. Creation, management and maintenance of one-time or recurring tracking/production reports, as required by AHCT to support activities outside the New Platform.

e. The selected Respondent must be able to perform all the aforementioned M&O services; however, AHCT reserves the right to contract with another vendor for some or all M&O services. The selected Respondent must work in conjunction with any such vendor to perform any activities or services related to the contracted M&O services.
f. A selected Respondent's Pricing Proposal must include separate, detailed pricing for the implementation services and the M&O services.

4. Key Personnel

    a. The selected Respondent's personnel should include, but are not limited to, Project Managers, ETL/Data Engineers, Data Architects, Report Developers, Security Architects, and at least one (1) UI Consumer Experience Lead.

5. Common health insurance terms used in this RFP are defined in AHCT's glossary of terms, available at: https://www.accesshealthct.com/glossary/.

3. ALIGNMENT TO EXCHANGE REQUIREMENTS

A Respondent must complete the Requirements Traceability Matrix (RTM) grids in **Appendix B** to indicate their proposed Solution's level of fit with specific Exchange requirements.

A Respondent will be required to submit a completed set of RTM grids as part of its Proposal:

- The Respondent will perform a self-assessment on its ability to meet requirements.
- For each subsection outlined, the Respondent must indicate, using the below descriptors, how its proposed capabilities meet the Exchange's requirements.
- The Exchange will assume that any requirement in an RTM grid that the Respondent fails to respond to cannot be met by Respondent.

A Respondent must use the following descriptors to describe its ability to meet requirements:

Meets the Requirement "MTR"	Meets all requirements as written in the sub-section (e.g., well-defined support system, flexibility, considerable implementation experience, has performed function in previous capacity)
Requires minor modification "RMM"	Demonstrates capabilities to meet requirements with slight adjustments (e.g., well-defined approach/plan to meet requirements with adjustments, performed similar but not exact function in past projects).
Requires significant modification "RSM"	Current Respondent's standard configuration does not demonstrate capabilities to meet requirements as written (e.g., insufficient support, no functionality built to meet requirement) and would have to make major changes in order to comply.
Does not comply or unable to deliver capability "DNC"	Not able to comply - or - No capability - or - No response provided

4. PRICING PROPOSAL

Respondents to this RFP must include a separate, detailed Pricing Proposal and a rate card in the format specified below. We require that the submitted Pricing Proposal follows the cadence and categories outlined in the tables below.

Additionally, the Pricing Proposal must include, for reference, a rate card with specific hourly rates for each category of employee who will provide the services described herein (excluding clerical staff), in the event that the Exchange requires additional contracted services that are not set forth in this RFP.

A selected Respondent's Pricing Proposal must include separate, detailed pricing for the implementation services, maintenance and operation services, and any value-added services. Please include any relevant narrative describing the breakdown of costs included in the Pricing Proposal.

The Pricing Proposal should reflect any discounted rates available to government, non-commercial, or not-for-profit entities.

All rates and pricing must be represented in U.S. Dollars.

The Pricing Proposal must be sent separately via email to Sinisa Crnkovic (Sinisa.Crnkovic@ct.gov) no later than 4:00 p.m. EST on October 31, 2025.

Stability of Proposed Fees

Any rates and fee(s) set forth in the Pricing Proposal must be valid for the entire duration of the Contract.

Independent Price Determinations

In the Pricing Proposal, Respondents must warrant, represent, and certify the following:

1. The fees and costs proposed have been arrived at independently, without consultation, communication, or agreement for the purpose of restricting competition as to any matter relating to such process with any other organization or with any competitor.

2. Unless otherwise required by law, the Respondent has not knowingly disclosed quoted fees directly or indirectly to any other organization or to any competitor prior to the deadline for submission of the Proposal.

3. No attempt has been made, or will be made, by the Respondent to induce any other person or firm to submit or not to submit a Proposal for the purpose of restricting competition.

New Platform Design and Implementation Costs

The Pricing Proposal must specify the product type (e.g., a Software as a Service model, a custom build, a hybrid build, etc.).

	New Platform Design & Implementation Costs	Fee(s)	Hours (if applicable)
*	**[Specify product type in this field, as mentioned above (SaaS, Custom, or Hybrid]**		
1	**Labor Costs**: Labor costs associated with the overall project management, requirements elicitation, design, development, testing, and implementation of the proposed New Platform. If multiple phases of implementation are proposed, then the fee(s) for each phase must be stated separately.		
2	**Hardware and Software Costs**: Hardware and software costs associated with design, development, and implementation of the proposed New Platform. Each component must be separately listed and priced. Pricing must reflect any environment hosting, procurement, and licensing costs. If multiple phases of implementation are proposed, then the fee(s) for each phase must be stated separately.		
3	**New Platform Training Costs**: Labor costs associated with creation of training materials and delivery of any and all requested 'Train-the-Trainer' sessions. If multiple phases of training are proposed, then the fee(s) for each phase must be stated separately.		
4	**New Platform Scanning**: Labor, hardware and software costs associated with the execution, reporting, and monitoring of environment and code scans, as specified in the Requirements Traceability Matrix. One-time and recurring costs must be stated separately.		
5	**Data Migration Start-up and Transition Costs**: Costs associated with the conversion/migration of all customer, eligibility, and enrollment data from the current HIX Platform to the proposed New Platform.		

6	**<u>Documentation Management</u>**: One-time costs associated with the development and delivery of a repository of documentation and manuals for the proposed New Platform. These deliverables include, but are not limited to, the deliverables outlined in Section 2 (“Scope of Work”) of this RFP.		
	<u>TOTAL IMPLEMENTATION COSTS</u>:		

<u>Ongoing Maintenance and Operations</u>

	Ongoing Maintenance and Operations Costs	Year 1 Fee(s)	Year 2 Fee(s)	Year 3 Fee(s)	Cumulative 3-Year Cost
1	**<u>Labor Costs</u>**: Labor costs associated with the post-implementation support of the proposed New Platform. Costs should include: monitoring and maintenance of environments/hardware, triage of production incidents, root cause analysis (RCA), and resolution planning and implementation.				
2	**<u>Hardware and Software Costs</u>**: Ongoing costs associated with the running and maintenance of the proposed New Platform and related environments. Each component must be separately listed and priced. Pricing must reflect any environment hosting, procurement, and licensing costs.				
3	**<u>Change Management:</u>** Costs associated with the planning, design, development, testing, and implementation of new or enhanced functionality, as identified by AHCT. Please include a rate card and preferred methodology: fixed price or time and materials.				
4	**<u>Documentation Maintenance</u>**: Labor costs associated with maintaining the documentation related to the proposed New Platform, including				

	but not limited to: requirements, functional design, technical design and architecture, user guides, training materials, business rules, and configuration.				
	TOTAL ONGOING MAINTENANCE AND OPERATIONS COSTS:				

Value-Added Services (If Any)

	Value-Added Costs (If Applicable)	Year 1 Fee(s)	Year 2 Fee(s)	Year 3 Fee(s)	Cumulative 3-Year Cost
1	**One-time Labor Costs**: One-time labor costs associated with any value-added service(s) or feature(s) submitted as part of the Proposal. Each value-added service or feature must be stated separately.				
2	**One-time Hardware and Software Costs**: One-time costs associated with the hardware and/or software related to any value-added service(s) or feature(s) submitted as part of the Proposal. Each value-added service or feature must be stated separately.				
3	**Ongoing Labor Costs**: Ongoing labor costs associated with any value-added service(s) or feature(s) submitted as part of the Proposal. Each value-added service or feature must be stated separately.				
4	**Ongoing Hardware and Software Costs**: Ongoing costs associated with the hardware and/or software related to any value-added service(s) or feature(s) submitted as part of the Proposal. Each value-added service or feature must be stated separately.				

	TOTAL VALUE-ADDED SERVICES COSTS:				

5. INSTRUCTIONS TO RESPONDENTS

I. RFP Schedule

Activity	Date
Issuance of RFP	9/23/2025
Written Questions Due	10/6/2025 by 4:00 p.m. EST
Answers Posted	10/17/2025
Proposals Due	10/31/2025 by 4:00 p.m. EST
Presentations	TBD

Respondents may submit written questions regarding this RFP by email only to RFP_HIXPlatformDevelopment@ct.gov no later than 4:00 p.m. EST on October 6, 2025. The Exchange will post answers on October 17, 2025, only in the form of one or more addenda to this RFP and made available on the Exchange's website, https://agency.accesshealthct.com/solicitations, under the "Contact Us" tab beneath the "Solicitations" heading. The Exchange may not post answers to questions received after the deadline. Respondents are responsible for checking the Exchange's website for any addenda to this RFP.

The Exchange reserves the right to require a presentation from select Respondents. If the Exchange moves forward with presentations, selected Respondent's key staff, such as the proposed project partner, must be present at the presentation. Selected Respondents should limit their staff participation to no more than five (5) members.

From the date that the Exchange issues this RFP until the date that it awards the Contract to the selected Respondent, interested firms or individuals should not contact any employee of the Exchange for additional information concerning this RFP except through written questions as set forth above.

II. Submission of Proposals

Note: Unless otherwise noted, references to "Proposal" includes "Pricing Proposal."

Each Respondent must submit a Proposal that meets the requirements set forth in the "Contents of Proposals" subsection below.

- Respondents must email their Proposal excluding the pricing Proposal to: Yessenia Milan (RFP_HIXPlatformDevelopment@ct.gov). The Subject line of the email should read: Health Insurance Exchange Integrated Eligibility and Enrollment Platform RFP Proposal – [Your Firm's Name].

- Respondents must email their Pricing Proposal to: Sinisa Crnkovic (Sinisa.Crnkovic@ct.gov). The Subject line of the email should read: Health Insurance Exchange Integrated Eligibility and Enrollment Platform RFP Pricing Proposal – [Your Firm's Name].

All Proposals must be received by the Exchange via e-mail by October 31, 2025, no later than 4:00 p.m. EST. Proposals sent by U.S. Mail or delivered in person will not be accepted. The Exchange will not consider Proposals received after the submission deadline.

A Respondent's submission of a Proposal shall constitute, without any further act required of the Respondent or the Exchange, the Respondent's acceptance of the requirements, administrative stipulations and all the terms and conditions of this RFP, including those contained in the Contract set forth in **Appendix C**. Proposals must reflect compliance with these requirements. Failure of a Proposal to so comply may result in the Exchange's rejection of the Proposal. The Exchange will reject any Proposal that deviates materially from the specifications, terms, or conditions of this RFP. The Exchange will not consider Proposals that contain even minor or immaterial deviations unless the Respondent provides sufficient justification for such deviations.

No additions or changes to any Proposal will be allowed after the Proposal due date unless the Exchange specifically requests the addition or change. The Exchange may, at its option, seek Respondent retraction and/or clarification of any discrepancy or contradiction found during the review of Proposals.

III. Contents of Proposals

To be considered, a Proposal must include all of the following:

1. Cover Letter, Table of Contents, and Executive Summary.

2. All information and responses requested by this RFP (including those in Section 3 ("Alignment to Exchange Requirements") and the "Responses Required in the Proposal" subsection below). Concise answers are encouraged. Responses must be prepared on 8 ½ x 11-inch paper using at least 12-point font type with standard margins in a PDF format.

3. A Certificate of Insurance that meets the Insurance requirements laid out in section 9 of the Contract, attached to the RFP as **Appendix C**. Alternatively, a Proposal can include a signed statement stating that the Respondent agrees to obtain all of the required insurance coverage it does not presently have prior to the execution of the Contract.

4. Executed IRS Form W-9.

5. Executed Ethics Form 1 – Campaign Contribution Certification, attached to the RFP as **Appendix D**.

6. Offer of Gratuities Certification (see Subsection X. below).

7. Validation of Proposal and Pricing Proposal (see Subsection XI. below).

IV. Responses Required in the Proposal

1. Name the primary contact for the Proposal and the names of the primary individuals who would work with the Exchange, and an explanation of their experience, relevant background, and anticipated duties. Include brief resumes for each.

2. Explain the firm's qualifications and provide a summary of any past projects that would enable your firm to perform the work described in Section 2 ("Scope of Work").

3. Disclose any past or present assignments, relationships, or other employment that your firm or any employee of your firm has or has had that may create a conflict of interest or the appearance

of a conflict of interest in serving as an independent contractor for the Exchange.

4. If you find any term or provision of the proposed draft Contract in **Appendix C** unacceptable, identify the term, explain why it is unacceptable, and state whether the failure to modify this term would result in your firm's failure to execute a contract for this engagement. If possible, please propose alternative language for any such term(s). *Please note, the terms in Exhibit B to the Contract and the required representations and certifications in Appendix A to the Contract cannot be altered or modified pursuant to Connecticut state law.*

5. Discuss any pending complaints or investigations, or any made or concluded within the past five (5) years, to or by any regulatory body or court regarding the conduct of your firm or its predecessors, or any of its present or former members, employees, attorneys and/or associates.

6. Provide a separate detailed Pricing Proposal in accordance with the requirements set forth in Section 4 ("Pricing Proposal").

7. Provide three (3) client references. Include the reference's name, company or organization, title, telephone number, email address, a description of the work performed (should be reasonably comparable to services sought in this RFP), and the dates of the work performed.

V. Conformity and Completeness of Proposals

To be considered acceptable, Respondents must submit Proposals that are complete and conform to all material RFP instructions and conditions. The Exchange, in its sole discretion, may reject in whole or in part, any Proposal if in its judgment the best interests of the Exchange will be served.

VI. Presentation of Supporting Evidence

Respondents must be prepared to provide evidence of experience, performance, ability, financial resources, or other items that the Exchange deems necessary or appropriate concerning the performance capabilities represented in their Proposals.

VII. Misrepresentation or Default

The Exchange may reject a Proposal and void any award resulting from this RFP to a Respondent that makes any material misrepresentation in its Proposal or other submission in connection with this RFP.

VIII. Disqualification

Any attempt by a Respondent to influence a member of the evaluation committee during the Proposal review and evaluation process will result in the elimination of that Respondent's Proposal from consideration.

IX. Oral Agreement or Arrangements

Any alleged oral agreements or arrangements made by Respondents with any state agency, the Exchange, or an employee of a state agency or the Exchange will be disregarded in any Proposal evaluation or associated award.

X. Offer of Gratuities

Respondents must certify that no elected or appointed official or employee of the State of Connecticut or the Exchange has, or will, benefit financially or materially from the Contract. The Contract may be terminated by the Exchange if it is determined that gratuities of any kind were either offered to, or received by, any of state officials or employees from the Respondent, the Respondent's agent(s), representative(s), or employee(s). Such action on the part of the Exchange shall not constitute a breach of contract by the Exchange.

XI. Validation of Proposals

Each Proposal (including each Pricing Proposal) must be signed by an authorized official and shall be a binding commitment that the Exchange may incorporate, in whole or in part, by reference or otherwise, into the Contract. The Proposal must also include evidence that the person submitting the Proposal has the requisite power and authority on behalf of the firm to submit and deliver the Proposal and subsequently to enter into, execute and deliver, and perform the Contract.

6. ADDITIONAL TERMS AND CONDITIONS

I. Ownership of Proposals

All Proposals (including Pricing Proposals) will become the sole property of the Exchange and will not be returned.

II. Amendment or Cancellation of this RFP

Issuance of this RFP does not guarantee that the Exchange will award a Contract to any Respondent. The Exchange reserves the right to withdraw, re-bid, extend or otherwise modify the RFP or the related schedule and process, in any manner, solely at its discretion.

The Exchange also reserves the right to:

- Consider any source of information in evaluating Proposals;
- Omit any planned evaluation step if, in the Exchange's view, the step is not needed;
- At its sole discretion, reject any or all Proposals at any time; and
- Open contract discussions with other Respondent(s) if the Exchange and the first selected Respondent is unable to agree on contract terms.

III. Errors

The Exchange reserves the right to correct clerical or administrative errors that may be made during the evaluation of Proposals or during the negotiation of the Contract and to change the Contract award accordingly. In addition, the Exchange reserves the right to re-evaluate Proposals and the award of the Contract in light of information either not previously known or otherwise not taken into account prior to the Contract award. This may include, in extreme circumstances, revoking the awarding of the Contract already made to a Respondent and subsequently awarding the Contract to another Respondent.

Such action on the part of the Exchange will not constitute a breach of contract on the part of the Exchange since the Contract with the initial Respondent would be deemed void and of no effect as if no contract ever existed between the Exchange and such Respondent.

The Exchange may waive minor irregularities found in Proposals or allow a Respondent to correct them, depending on which is in the best interest of the Exchange. "Minor irregularities" means typographical errors, informalities that are matters of form rather than substance and evident from the Proposal itself, and insignificant mistakes that can be waived or corrected without prejudice to other Respondents, as determined in the sole discretion of the Exchange.

IV. Freedom of Information

The Exchange is a quasi-public agency and its records, including responses to this RFP, are public records. *See* Conn. Gen. Stat. §§ 1-200, *et seq*., and especially §§ 1-210(b)(4) and 1-210(b)(5)(B). Due regard will be given to the protection of proprietary or confidential information contained in all Proposals received. All materials associated with this RFP, however, are subject to the terms

of the Connecticut Freedom of Information Act ("FOIA") and all applicable rules, regulations, and administrative decisions. If a firm is interested in preserving the confidentiality of any part of its Proposal, it will not be sufficient merely to state generally in the Proposal that the Proposal is proprietary or confidential in nature and not, therefore, subject to release to third parties. Instead, the firm must specifically identify those particular sentences, paragraphs, pages, or sections that a firm believes to be exempt from disclosure under FOIA. Convincing explanation and rationale sufficient to justify each exemption consistent with § 1-210(b) of FOIA must accompany the Proposal. Any submitted Proposal and the fully executed Contract will be considered public information and subject to FOIA. The Exchange has no obligation to initiate, prosecute or defend any legal proceeding or to seek a protective order or other similar relief to prevent disclosure of any information that is sought pursuant to a FOIA request. The firm has the burden of establishing the availability of any FOIA exemption in any proceeding where it is an issue. In no event shall the Exchange have any liability for the disclosure of any documents or information in its possession that the Exchange believes are required to be disclosed pursuant to FOIA or any other law.

V. Statutory and Regulatory Compliance

By submitting a Proposal in response to this RFP, the Respondent implicitly agrees to comply with all applicable State and federal laws and regulations, including, but not limited to, the following:

A. **Gifts, C.G.S. § 4-252.** Pursuant to section 4-252 of the Connecticut General Statutes and Acting Governor Susan Bysiewicz's Executive Order No. 21-2, the Contractor, for itself and on behalf of all of its principals or key personnel who submitted a bid or proposal, represents:

1. That no gifts were made by (A) the Contractor, (B) any principals and key personnel of the Contractor, who participate substantially in preparing bids, proposals or negotiating State contracts, or (C) any agent of the Contractor or principals and key personnel, who participates substantially in preparing bids, proposals or negotiating State contracts, to (i) any public official or State employee of the State agency or quasi-public agency soliciting bids or proposals for State contracts, who participates substantially in the preparation of bid solicitations or requests for proposals for State contracts or the negotiation or award of State contracts, or (ii) any public official or State employee of any other State agency, who has supervisory or appointing authority over such State agency or quasi-public agency;

2. That no such principals and key personnel of the Contractor, or agent of the Contractor or of such principals and key personnel, knows of any action by the Contractor to circumvent such prohibition on gifts by providing for any other principals and key personnel, official, employee or agent of the Contractor to provide a gift to any such public official or State employee; and

3. That the Contractor is submitting bids or proposals without fraud or collusion with any person.

B. **Campaign Contribution Restriction, C.G.S. § 9-612.** For all State contracts, defined in section 9-612 of the Connecticut General Statutes as having a value in a calendar year of $50,000 or more, or a combination or series of such agreements or contracts having a value of $100,000 or more, the authorized signatory to the resulting contract must represent that they have received the State Elections Enforcement Commission's notice advising state contractors of state campaign contribution and solicitation prohibitions, and will inform its principals of the contents of the notice, as set forth in "Notice to Executive Branch State Contractors and Prospective State Contractors of Campaign Contribution and Solicitation Limitations." Such notice is available at:

https://seec.ct.gov/Portal/data/forms/ContrForms/seec_form_11_notice_only.pdf

C. **Contract Compliance, C.G.S. § 4a-60 and Regulations of CT State Agencies § 46a-68j-21 through § 46a-68j-43, inclusive.** Connecticut statutes and regulations impose certain obligations on the Exchange (as well as contractors and subcontractors doing business with the State) to ensure that the Exchange does not enter into contracts with organizations or businesses that discriminate against protected class persons.

D. **Consulting Agreements Representation, C.G.S. § 4a-81.** Pursuant to C.G.S. § 4a-81, the successful Respondent shall certify that it has not entered into any consulting agreements in connection with this Contract, except for the agreements listed in the Contract form. "Consulting agreement" means any written or oral agreement to retain the services, for a fee, of a consultant for the purposes of (A) providing counsel to a contractor, vendor, consultant or other entity seeking to conduct, or conducting, business with the State, (B) contacting, whether in writing or orally, any executive, judicial, or administrative office of the State, including any department, institution, bureau, board, commission, authority, official or employee for the purpose of solicitation, dispute resolution, introduction, requests for information, or (C) any other similar activity related to such contracts. "Consulting agreement" does not include any agreements entered into with a consultant who is registered under the provisions of chapter 10 of the Connecticut General Statutes as of the date such contract is executed in accordance with the provisions of section 4a-81 of the Connecticut General Statutes. Such representation shall be sworn as made to the best knowledge and belief of the person signing the resulting contract and shall be subject to the penalty of false statement as provided in C.G.S. § 53a-157b.

E. **Nondiscrimination Certification, C.G.S. § 4a-60 and § 4a-60a.** If a Respondent is awarded an opportunity to negotiate a contract, the Respondent must provide the Exchange with *written representation* in the resulting contract that certifies the Respondent complies with the State's nondiscrimination agreements and warranties. This nondiscrimination certification is required for all State contracts – regardless of type, term, cost, or value. Municipalities and CT State agencies are exempt from this requirement. The authorized signatory of the contract shall demonstrate his or her understanding of this obligation by (A) initialing the nondiscrimination affirmation provision in the body of the resulting contract, (B) signing the resulting contract, or (C) providing an affirmative response in the required online bid or response to a proposal question, if applicable, which asks if the contractor understands its obligations.

F. **Iran Energy Investment Certification.**

(a) Pursuant to section 4-252a of the Connecticut General Statutes, the successful Respondent must certify that it has not made a direct investment of twenty million dollars or more in the energy sector of Iran on or after October 1, 2013, as described in Section 202 of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010, and has not increased or renewed such investment on or after said date.

(b) If the Respondent makes a good faith effort to determine whether it has made an investment described in subsection (a) of this section, it shall not be deemed to be in breach of the contract or in violation of section 4-252a of the Connecticut General Statutes. A "good faith effort" for purposes of this subsection includes a determination that the Respondent is not on the list of persons who engage in certain investment activities in Iran created by the Department of General Services of the State of California pursuant to Division 2, Chapter 2.7 of the California Public Contract Code.

G. **Access to Data for State Auditors**. The Contractor shall provide to the Exchange access to any data, as defined in C.G.S. § 4e-1, concerning the resulting contract that are in the possession or control of the Contractor upon demand and shall provide the data to the Exchange in a format prescribed by the Exchange and the State Auditors of Public Accounts at no additional cost.

If the selected Respondent does not agree to the representations required under this section, it shall be rejected, and the Exchange shall award the Contract to the next highest ranked Respondent.

IV. Execution of Contract

This RFP is the instrument through which the Exchange solicits Proposals. This RFP is not a contract. Upon the Exchange's selection of a Respondent, the Respondent must enter into a contract with the Exchange substantially in the form of the Contract set out in **Appendix C**. The selected Respondent's Proposal and this RFP may serve as the basis for additional Contract terms. If the Exchange and selected Respondent fail to reach an agreement on Contract terms within a time determined solely by the Exchange, then the Exchange may commence and conclude contract negotiations with other Respondents. The Exchange may decide at any time to start this RFP process again.

V. Subletting or Assigning of Contract

The Contract or any portion thereof, or the work provided for therein, or the right, title, or interest of the Respondent therein or thereto may not be sublet, sold, transferred, assigned, or otherwise disposed of to any person or entity without the prior written consent of the Exchange. No person or entity, other than the Respondent to which the Contract was awarded, is permitted to perform work without the prior written approval of the Exchange.

VI. Compliance with Federal, State and Other Requirements

In the Contract, the Respondent will represent and warrant that, at all pertinent and relevant times to the Contract, it has been, is and will continue to be in full compliance with all codes, statutes, acts, ordinances, judgments, decrees, injunctions, and regulations of federal, state,

municipal or other governmental departments, commissions, boards, bureaus, agencies, or instrumentalities.

VII. Executive Orders

The Contract shall be subject to the provisions of Executive Order No. Three of Governor Thomas J. Meskill, promulgated June 16, 1971, the provisions of Executive Order No. Seventeen of Governor Thomas J. Meskill, promulgated February 15, 1973, and the provisions of Executive Order No. Sixteen of Governor John G. Rowland promulgated August 4, 1999.

APPENDICES

APPENDIX A – HIX PLATFORM MODERNIZATION

APPENDIX B – REQUIREMENTS TRACEABILITY MATRIX

APPENDIX C – INDEPENDENT CONTRACTOR AGREEMENT

APPENDIX D – ETHICS FORM 1: GIFT AND CAMPAIGN CONTRIBUTION CERTIFICATION

APPENDIX A

HIX PLATFORM MODERNIZATION

HIX Platform Modernization

Introduction

For years, Access Health CT's application ecosystem has been supported through a traditional delivery model: monolithic applications, hosted on-premises, and developed by external implementation partners who managed source code and database logic in their own repositories and delivered compiled artifacts and SQL scripts to our internal teams. This model has served its purpose but is no longer aligned with the demands of scalability, agility, and governance expected of a modern public health platform.

In this legacy setup, our internal App hosting infrastructure and DBA teams are responsible for deploying partner-supplied application binaries and SQL scripts into tightly controlled environments. A separate vendor executes testing, and maintenance is handled by yet another, resulting in a highly siloed and coordination-intensive operational landscape. These divisions, while necessary, have unintentionally eroded **internal visibility and control** across the application lifecycle, from code inception to production deployment.

This modernization initiative is not just about moving workloads to the cloud. It is about **redefining the entire software delivery model**, and more importantly, **reclaiming ownership** of our platform's operational and architectural integrity, without sacrificing the ability to continue engaging external partners for development, testing, and support.

We are shifting from a **vendor-driven model** to a **platform-driven model**:

- One where **Access Health CT owns the infrastructure, environments, source code, security boundaries, and delivery pipelines**;
- And **external vendors are integrated through secure, auditable, and standardized workflows** that align with our internal governance, and don't bypass it.

This document lays out the **comprehensive, end-to-end workflow** that enables this transformation. It begins at the foundation — with cloud-native environment provisioning — and moves upward through source code management, CI/CD, infrastructure and app deployments, database modernization, monitoring, compliance, partner access control, and ultimately, full observability into platform health and delivery metrics.

Our internal **DevOps team serves as the enabling platform organization**, providing tools, environments, and delivery patterns that empower vendors to deliver while ensuring that all activities remain visible and adhere to **our governance policies.**

This approach allows Access Health CT to:

- Maintain **strong security, compliance, and audit trails**
- Accelerate release cycles with **automation and repeatability**
- Create **per-partner, per-project environment isolation** without operational overhead
- Ensure **every application and database change** is traceable, tested, and observable from the moment it is committed to the moment it reaches production.

This document serves as a **technical blueprint** and a **living guide** for how we expect modernization partners to work with us going forward. While we welcome partner expertise, we expect future vendors to work **within our platform model**, not around it. Let's now walk through each part of this modernized delivery lifecycle from infrastructure provisioning to monitoring and continuous improvement.

Target Architecture Overview

Access Health CT's modernization strategy is rooted in a fundamental shift: we are moving from a legacy model — where the platform is **shaped by vendors** — to a new model, where the platform is **defined, controlled, and evolved in-house**, while enabling vendors to participate securely and effectively through our delivery infrastructure.

This section defines the **target architecture** that will support this new operating model. It is not just a technology blueprint, but an operational foundation that allows Access Health CT to balance **control, flexibility, and accountability** across multiple vendors, without losing velocity or innovation.

This architecture is designed to:

- **Decouple** infrastructure and deployment from any single vendor or technology stack
- **Standardize** delivery and operational processes across all application domains
- **Scale horizontally** as vendor count, application modules, and environments grow
- **Support incremental modernization**, including coexistence with legacy systems
- **Automate enforcement** of security, compliance, and quality standards
- **Provide transparency and visibility** at every stage of the application lifecycle

Logical Architecture Layers

The architecture is built on five logical layers, each serving a distinct purpose but integrated into a unified workflow. These layers serve as the **shared delivery backbone** for internal teams and all participating vendors.

Infrastructure Platform Layer

This is the foundational layer that defines **how environments are created, secured, and managed**. It includes:

- Cloud networking, compute, storage, IAM, DNS
- Role- and project-based segmentation
- Shared services such as secrets management, logging, telemetry, and policy enforcement

All infrastructure is **declaratively defined using Infrastructure as Code**, versioned, and provisioned through CI/CD pipelines. Vendors are never given direct control over infrastructure — they operate **within boundaries that we define**, using tools and templates that we manage.

Application Delivery Layer

This layer governs how code moves from developer branches to production. It consists of:

- CI/CD pipelines
- Artifact repositories
- Deployment orchestration
- Release validation
- Promotion logic across environments (dev → test → UAT → prod)

Partners do not define their own CI/CD pipelines from scratch. Instead, they plug into pre-established pipeline templates with opinionated defaults, maintained by our DevOps team. These templates include **quality gates, security scans, approvals, and rollback logic** by default.

Source Code and Configuration Layer

All application source code, infrastructure code, and configuration live in **centrally hosted, Access Health CT–owned repositories**. Vendors are granted access to specific repositories or modules based on role and scope. Key principles:

- **Central ownership, federated contribution**
- **Branch-based workflows** with enforced pull request reviews

- Integration of **policy-as-code**, secrets scanning, and static analysis into the commit pipeline

This model ensures that every change, regardless of who authored it, is subject to the same review and compliance standards.

Runtime Execution Layer

This represents the deployed application and database workloads across various environments. These can include:

- Deployed containers or VMs in a Public cloud environment.
- Shared middleware and API gateways
- Scalable backend databases
- Per-vendor dev/test sandboxes
- Network segmentation and perimeter isolation

The internal team manages lifecycle operations, and vendors interact through controlled deployment triggers or temporary access boundaries.

Observability and Operations Layer

To support transparency and accountability, we maintain centralized systems for:

- Logs, metrics, traces
- Uptime monitoring, threshold alerts
- Per-service health dashboards
- Deployment and pipeline telemetry

Both internal teams and vendor teams will have scoped, read-only access to dashboards and logs relevant to their domains. No system is considered fully delivered unless it emits usable telemetry.

Environment Strategy

We define multiple **environment types**, each with distinct operational characteristics:

Environment	Purpose	Access Control
Dev	Rapid iteration, feature development	Partner-specific access

Environment	Purpose	Access Control
Test/UAT	Validation and QA	Cross-partner shared
Stage	Pre-prod testing with production-like configurations	Internal use + limited vendor visibility
Prod	Live workloads	Internal-only deployment control

Additionally, vendors may be allocated **ephemeral sandboxes**, created on demand through automation, with fixed expiration dates and scoped IAM policies.

No vendor will have persistent access to any environment unless explicitly granted. All access is logged, time-bound, and compliant with policy.

Modernization-Friendly Design

This architecture is not designed to force a big-bang rewrite. We are embracing **coexistence** and **progressive modernization** through:

- **The Strangler Pattern**: Gradually decompose monoliths by externalizing capabilities into discrete services
- **Adapter Layers**: Create façade APIs around legacy systems to isolate downstream consumers
- **Dual-Write and Sync**: For stateful systems, ensure safe transition by synchronizing data between old and new
- **Legacy Wrappers**: Legacy applications will continue running in the short term, but under improved observability and delivery control

By designing the platform to support both **new and existing features** side by side, we create an upgrade path that is practical, auditable, and aligned with partner bandwidth.

Operational Model for Multi-Vendor Support

Key to our approach is enabling vendors to work **autonomously within controlled boundaries**. Our DevOps team will function as a **Platform Engineering team**, responsible for:

- Building and maintaining reusable CI/CD and IaC templates
- Provisioning new environments and sandboxes on demand
- Managing access delegation and revocation
- Providing audit trails, metrics, and operational dashboards

- Enforcing security controls without obstructing productivity

Each vendor will:

- Work from centrally hosted repositories
- Use a defined branching and pull request model
- Trigger or request deployments via automated pipelines
- Receive scoped visibility into logs, errors, and test results
- Operate within contractual SLAs enforced via tooling

This model fosters **vendor accountability**, **delivery speed**, and a robust **security posture,** all without compromising control.

Current Access Health CT Tools and Practices (For Reference Only)

While the architecture is intentionally vendor-agnostic, here are some tools that Access Health CT currently utilizes to support these workflows. The following tools are only provided as examples:

Capability	**Example Tools**
Infrastructure as Code	**Terraform**, CloudFormation with AWS/Azure public cloud platform
CI/CD	**GitHub Actions**, Jenkins, Argo Workflows
Secrets Management	Vault, **AWS Secrets Manager**, SOPS
Deployment Orchestration	ArgoCD, Spinnaker, **Helm**
Observability	**New Relic**, Prometheus, Grafana, ELK Stack, Datadog
Source Repositories	**GitHub Enterprise Cloud**, GitLab
Access & Identity	**SSO w/ OIDC**, **AWS IAM**, Azure AD, custom role delegation services

Infrastructure Provisioning and Management

Access Health CT's future state infrastructure strategy is built on two core principles:

1. **Infrastructure is code** — every environment, subnet, compute node, database, and IAM policy must be defined, versioned, and reproducible through declarative configuration
2. **Environments are ephemeral, isolated, and vendor-controlled only through delegation** — no vendor should ever own infrastructure directly; instead, they must be able to work independently *within* controlled boundaries.

This section outlines how our internal DevOps team provisions, structures, governs, and manages environments to strike a balance between **speed, control, and security** across multiple internal and external delivery teams.

Environment Strategy and Classification

Each environment serves a specific purpose in the software delivery lifecycle. These are not simply copies of each other — they are **intentionally distinct** in terms of their access, auditability, and operational constraints.

Environment	Purpose	Ownership	Access Scope	Lifespan
dev	Partner-led feature development, local integration	Internal DevOps	Partner specific (scoped access)	Long-lived
test/QA	Centralized testing, partner coordination	Internal QA + DevOps	Cross-partner	Long-lived
stage/UAT	Business acceptance testing	Internal QA + DevOps	Internal + limited vendor	Long-lived
prod	Production workloads	Internal Infra + SRE	No vendor access	Permanent
sandbox	Isolated, ad hoc envs for individual partner work	DevOps (auto-provisioned)	Single partner only	Ephemeral (1–14 days)

Each environment is **infrastructure-as-code-defined**, tagged by purpose and owner, and tracked as part of a centralized inventory. Ephemeral environments (e.g., partner sandboxes) are automatically spun up and torn down via pipeline workflows or self-service portals, which are gated by access policies.

Infrastructure as Code (IaC) Foundations

All provisioning is automated using **Infrastructure as Code (IaC)** tools, integrated with our source control and CI/CD pipeline tooling. Key characteristics:

- **Every resource** — VPCs, subnets, IAM policies, compute groups, storage, databases — is described in code.

- **Modular structure** — reusable environment templates abstract common patterns (e.g., API gateway + app + DB).
- **Git-based changes** — changes to infrastructure follow the same branching, PR, review, and approval process as application code.
- **State tracking** — environment states are stored securely, allowing for drift detection and recovery.

No infrastructure should be provisioned manually or through cloud console interfaces unless for break-glass emergency debugging (and only by authorized internal personnel).

Network, Access, and Isolation Design

Environments are **logically and physically isolated** through:

- Dedicated **VPCs** per environment class
- Separate **subnets** for public-facing services, backend apps, databases, and management interfaces
- **Per-partner segmentation**, allowing sandbox environments to have dedicated networking boundaries
- **Strict firewall, routing, and endpoint gateway controls**

Access into any environment follows **Just-in-Time (JIT)** and **least-privilege principles**:

- Internal engineers authenticate via SSO and role assumptions
- Vendor teams authenticate through federated identity roles mapped to specific environments or services
- All access is logged centrally and can be revoked at any time via IAM or pipeline rollback

Environment Lifecycle Workflows

The infrastructure lifecycle is managed through declarative workflows — meaning everything from **creation to teardown** is driven via pipelines and Git operations. Key workflows include:

New Environment Bootstrapping

Typical use case: DevOps creates a partner-specific sandbox or a new test environment for a project.

1. A DevOps engineer or automation pipeline triggers the env request
2. IaC templates are instantiated with tags, labels, resource class, and policy bindings
3. Networking, secrets, CI/CD runners, and default monitoring agents are provisioned
4. Access roles for the intended vendor team are created and scoped to the environment
5. CI/CD config and telemetry hooks are attached
6. Environment is added to the central catalog and visibility dashboards

Environment Updates and Patch Management

Typical use case: Modifying resource size, changing secrets, updating configurations

1. Change is proposed via Git PR against IaC modules
2. Auto-linter and policy-as-code tools validate compliance
3. Peer review and approval via standard code review process
4. CI pipeline runs plan + apply cycle
5. Change is tracked and audit-logged

Environment Teardown

Typical use case: Decommissioning ephemeral partner sandboxes post-delivery

1. Teardown triggered via Git or approval portal
2. CI pipeline confirms state, triggers backups, revokes credentials
3. Deletes all associated infra (compute, DB, IAM, networking)
4. Cleans up access tokens, inventory references, cost centers

Environment Metadata and Tagging

All environments are **tagged and labeled** consistently for visibility, cost tracking, security policy application, and automation. Standard tagging schema includes:

- env: dev, test, stage, prod, sandbox
- owner: internal team or partner ID
- project: application or initiative name
- expiry: auto-expiration date for ephemeral environments
- type: microservice, monolith, shared infra, DB, cache, etc.
- compliance-level: PHI, PII, unrestricted

These tags feed into dashboards, cost tools, and policy enforcement mechanisms. For example, environments with a compliance level of PHI are automatically scanned for encryption at rest, restricted subnets, and required audit logging.

Secrets, Identity, and Secure Parameter Injection

Secrets (API tokens, DB passwords, credentials) are never hardcoded or shared manually.

Instead:

- All secrets are injected at runtime through **secure secrets managers** (vault systems or parameter stores).
- Secrets are referenced in infrastructure and app deployments via **tokens or encrypted references.**

- Partner access to secrets is **scoped by role, namespace, and environment**, and is always revocable.
- Rotation policies are automated, with forced rotation triggers post-vendor offboarding.

Disaster Recovery and Environment Resilience

All infrastructure is deployed in a manner that supports high availability and recoverability:

- **Backups**: Enforced backup policies for DBs and stateful volumes.
- **Failover**: Where supported, environments can fail over to alternate zones/regions.
- **Rebuild ability**: Any environment must be able to be re-provisioned **from scratch using IaC alone** (no manual state dependencies).

Source Code Management (SCM) Strategy

At the heart of this modernization initiative is a clear and uncompromising principle: **Access Health CT owns all source code** — application, infrastructure, deployment, configuration, database — across the entire lifecycle.

This marks a deliberate departure from the legacy model, where implementation partners managed their own repositories and delivered compiled artifacts and SQL scripts. In the new architecture, all code lives in Access Health CT–managed version control systems. Partners contribute *to* that structure, never around it.

This section outlines how source code is structured, governed, and accessed, with specific emphasis on **branching strategies, contribution workflows, policy enforcement, and secure practices** that support our platform-first, vendor-inclusive delivery model.

Central Repository Ownership and Structure

All code across application domains, infrastructure, database schema, CI/CD pipelines, and test automation is stored in **centralized Git-based repositories**, hosted under Access Health CT's source control management system (e.g., GitHub Enterprise, GitLab, Bitbucket Server).

Repository Types:

Repo Category	Description
Application Repos	Business service source code (Java, JS, etc.) per domain
Infrastructure Repos	IaC code (Terraform, Pulumi), environment bootstraps, shared modules
Database Repos	Versioned schema definitions, migration scripts, rollback logic

Repo Category	Description
CI/CD Templates	Reusable GitHub Actions, GitLab CI files, deployment policies
Shared Libraries/SDKs	Internal utilities or cross-app frameworks
Documentation	Markdown-based developer guides, runbooks, SOPs

Repos are **scoped and segmented by domain and function**, not by vendor. Multiple vendors may contribute to the same repository, but within **guardrails** we control.

Branching Model and Contribution Workflow

We enforce a standardized **branching and contribution model**, designed to balance parallel development needs with strict code hygiene, review, and traceability.

Primary Branches:

- main / master: Always production-ready
- release/*: Versioned staging branches used for pre-production testing
- dev: Integration branch for approved feature work before promotion

Feature Workflows:

- All vendors create branches from dev or release/* (depending on the delivery phase)
- Branch naming convention:

  feature/<vendor-id>/<jira-ticket>

  bugfix/<vendor-id>/<ticket-id>

Pull Requests:

- All code must be merged via pull requests (PRs)
- PRs trigger automated:
  - Linting
  - Static code analysis
  - Secrets scanning
  - Build & test execution
- A minimum of 1 internal reviewer approval is required
- Merge commits are disallowed; we enforce squash or rebase + fast-forward merges for clean history

Vendor Access and Permissions

Vendors are granted **scoped access** to specific repositories and branches through **role-based access controls (RBAC)** configured in the SCM platform.

Key Policies:

- No vendor has write access to main, release/*, or prod branches
- Vendors only have write access to:
    - Feature branches they created
    - Certain development branches, if authorized
- All write permissions are time-bound and revocable
- Repo activity (commits, PRs, comments) is audit-logged

This ensures that vendors can operate independently within defined boundaries but cannot impact production-critical branches or environments without oversight.

Secrets and Credential Handling

To eliminate the risk of accidental credential leaks or insecure commits:

- **No hardcoded secrets or keys are ever permitted** in source code
- Pre-commit hooks and CI scanners check for:
    - API keys
    - Passwords
    - Tokens
    - SSH keys
- Secrets are referenced via environment variables or secure vault references
- Any detected secret is auto revoked and reported to the internal security team

We also enforce automated credential rotation policies across all platforms that integrate with source-controlled infrastructure (e.g., database provisioning scripts or S3 access tokens in Terraform modules).

SCM Policy Enforcement and Automation

To ensure consistency and compliance across all contributions:

- **Branch Protection Rules**:
    - Prevent force pushes or deletions
    - Require signed commits on main, release/*
    - Require status checks (tests, policies) to pass before merge.
- **Code Owners and Review Mapping**:

    - Certain files/folders are auto-routed to internal teams for review
    - For example, /infra, /secrets, and /db/migrations must be reviewed by platform engineering or DBAs
- **Automated PR Templates**:
    - All PRs must use standardized templates, referencing JIRA IDs, context, risk level, and rollback plan
- **Integration with JIRA or Ticketing System**:
    - No PR is accepted without an approved JIRA ticket in appropriate status
    - Pipeline metadata links commits to business requests for traceability

Compliance, Traceability, and Audit

Access Health CT requires full traceability of who changed what, when, why, and how it was reviewed.

Our SCM platform is configured to:

- Retain commit histories, tags, and PR reviews indefinitely
- Link commits to identities via corporate SSO
- Generate periodic reports on:
    - Commit frequency by vendor
    - Code review SLA adherence
    - Branch lifecycle metrics
    - Secrets scanning alerts

This provides an audit trail suitable for both internal compliance and external reporting obligations.

Repository Lifecycle Management

To prevent sprawl and abandoned repositories:

- All repositories must have:
    - An assigned internal owner
    - A lifecycle policy (active, archived, deprecated)
    - Documentation minimum standards
- Orphaned branches are flagged and deleted after defined inactivity periods
- Repositories are regularly scanned for:
    - Unused files
    - Obsolete dependencies
    - High-risk commit patterns (e.g., large binaries or keys)

CI/CD Pipelines

The CI/CD (Continuous Integration and Continuous Deployment) layer is where automation, quality enforcement, and delivery velocity converge. This is the **engine that turns code into deployable, testable, observable applications** — without relying on manual handoffs, opaque approvals, or out-of-band deployment instructions.

In the future-state architecture, **Access Health CT owns the CI/CD platform**, defines the pipeline templates, and enforces the delivery contracts. Vendors contribute into this structure by pushing code or triggering builds, but they do not define the pipelines themselves. This ensures **consistency, auditability, and security** across all deployments whether performed by internal teams or external partners.

This section outlines how the CI/CD architecture is designed, governed, and executed — from build through deployment and rollback — across all environments and applications.

Design Principles

The CI/CD system is built around these key principles:

- **Everything-as-Code**: Pipelines, tests, environment configs, and deployment logic are versioned and stored in SCM
- **Pipeline Standardization**: All services follow consistent templates and deployment structures
- **Environment Promotion**: Artifacts are promoted through environments, not rebuilt
- **Security Gates & Audits**: Every pipeline stage includes automated and human review checkpoints
- **Observability and Traceability**: Every deployment is logged, version-tagged, and tied to commit IDs and JIRA tickets
- **No Manual Deployments**: All production deployments are initiated through pipeline triggers with policy-based approvals

Pipeline Stages (Logical Flow)

The standard CI/CD pipeline for every service or component includes the following stages:

1. Code Build

- Triggered on PR or merge to an integration branch
- Executes:
    - Dependency resolution
    - Compilation / transpilation
    - Linting

    - Static code analysis
- Output: Build artifacts (JAR, WAR, container image, ZIP, etc.)

2. Unit and Component Testing

- Framework-level unit tests
- Code coverage validation
- Pre-commit or PR-blocking thresholds enforced
- Runs in parallel containers or runners for speed

3. Security & Compliance Checks

- Secrets scanning
- SAST (Static Application Security Testing)
- License compliance (OSS scanners)
- Policy-as-Code hooks (e.g., required annotations, naming, tags)

4. Artifact Packaging & Signing

- Artifacts are:
    - Versioned using commit hash, timestamp, or semantic versioning
    - Signed (optional for critical services)
    - Stored in internal artifact registry
- Immutable artifact tagging guarantees that the same build is deployed across environments

5. Integration Testing & Quality Gates

- Deploys to short-lived test environments or mocks
- Executes:
    - API contract tests
    - Database migrations on dummy instance
    - UI smoke tests (if applicable)

6. Deploy to Dev / Sandbox

- Triggers deploy pipeline
- Pulls artifact from registry
- Runs infrastructure and application deploy together (IaC + App)
- Runs post-deploy health checks, telemetry setup, and environment tagging
- Notifications sent via Slack/email for success/failure

7. Promotion to QA / UAT / Stage

- Manually or automatically gated
- Promotion means reusing the **exact same artifact** built and stored earlier
- Optional performance, load, and regression tests run here
- Approval workflows built-in (JIRA ticket or manager sign-off)

8. Production Deployment

- Triggered via Git tag, release event, or change management ticket
- Includes:
    - Final approval gate
    - Lock window or change freeze check
    - Canary or blue-green deployment pattern (if supported by the app)
    - Automatic rollback hooks if health checks fail
    - Audit logging of approver, timestamp, and release notes

Vendor and Team-Specific Pipelines

Each partner or project team does **not own their own pipeline definition**. Instead, the DevOps team provides:

- **Reusable CI/CD templates** for different application types (Java, Node.js, containerized microservices, database migrations, etc.)
- **Shared CI/CD modules** for common functionality (e.g., artifact upload, DB validation, SAST scans)

Scenario	Vendor Responsibility	Platform Responsibility
App Build	Push code to vendor specific dev branch	CI builds, scans, notifies
DB Change	Add Liquibase changelog file to PR	Pipeline validates against dummy DB
Test Execution	Add test suite to repo	Test runner executes & stores results
Deployment	Tag or request deploy	CD pipeline deploys to target env with logs

Approval and Compliance Integration

To enforce change management without introducing bureaucracy, we integrate approvals directly into the pipeline:

- **Automated checks** for:
    - Required approvals

    - Ticket validation
    - Reviewer identity
- **Manual approval steps** using:
    - SCM-based “required reviewer” model
    - Slack-based bot approvals
    - Web portals integrated with change control systems

Pipeline metadata (commit ID, ticket ID, approver, timestamp) is written to a central audit log and stored with the release record.

Observability and Notifications

Every pipeline execution emits logs, metrics, and events to the observability layer. Key events include:

- Build success/failure
- Test pass/failures
- Deployment durations
- Error rates post-deploy
- Regression indicators

Stakeholders are notified via:

- Slack / MS Teams
- Email digests
- Central dashboards

Dashboards are organized by team, app, environment, and vendor for full visibility.

Rollbacks and Recovery

All pipelines support automated and manual rollback paths:

- Application rollback: Deploy previous artifact
- Infrastructure rollback: Revert to last known-good IaC state
- Database rollback: Reverse Liquibase changelogs or apply rollback scripts (if available)

Rollback actions are tied to pipeline events and tracked in audit history.

Database Modernization and Change Management

Access Health CT’s modernization effort cannot succeed without transforming the way databases are managed. Our legacy model — where implementation partners authored raw

SQL scripts and submitted them to our in-house DBAs for manual execution — created bottlenecks, introduced operational risk, and made rollback and compliance tracking difficult.

In the new model, **databases are treated as first-class code artifacts**, subject to the same lifecycle and governance controls as application code. This means every schema change, migration, or data patch is tracked, versioned, tested, and deployed via pipelines — with no manual steps, no ambiguity, and no unreviewed access.

This section outlines the end-to-end strategy for modern, secure, and auditable database change management that can support a **multi-vendor development model**, while ensuring that **Access Health CT retains full control over data, change cadence, and security posture**.

Key Principles

The modern database strategy is governed by the following foundational principles:

- **Declarative, Versioned Changes**: Schema and data changes are defined as code, stored in SCM, and versioned
- **No Manual Execution**: DBAs do not manually run scripts; all changes flow through CI/CD pipelines
- **Environment-Aware Changes**: Changes are validated and applied per environment, with rollback hooks
- **Auditability**: Every DB change is linked to a ticket, commit, PR, and deployment
- **Vendor Contribution with Guardrails**: Partners can propose DB changes, but cannot bypass internal review or promote without approval

Repository Structure and Ownership

Each application repository includes a structured directory for database migrations:

```
/db
 /changelog
  - V001__create_users_table.sql
  - V002__add_index_to_email.sql
  - V003__add_payment_flag_column.sql
 /rollback
  - R001__drop_users_table.sql
  - R002__remove_email_index.sql
 /reference
  - full_schema_snapshot.sql
 /data
  - seed_users_data.sql
```

All files are:

- Stored in SCM under Access Health CT's Git org
- Reviewed through PRs with appropriate ownership (e.g., DBAs or platform team)
- Referenced by CI/CD pipelines for plan/apply/rollback cycles

Migration Tools and Execution Flow

We standardize all migrations through **a versioned migration tool** (e.g., Liquibase, Flyway, Alembic) embedded into the CI/CD pipeline.

Typical Workflow:

1. **Vendor adds migration script** to /db/changelog and submits a PR
2. **PR triggers CI**:
    - Syntax and structure validation
    - Migration dry-run on a scratch DB or container
    - Validation against schema snapshot
3. **Reviewers (DBAs/Platform)** approve or reject
4. **On merge**, CD pipeline promotes the migration to the target environment:
    - Creates DB backup (if supported)
    - Applies migration
    - Runs post-migration tests or triggers synthetic health checks
5. **Post-deploy artifacts** (SQL logs, success/failure flags, timestamps) are stored with the release record.

Change Categorization

Changes are categorized to improve review and rollback processes:

Category	Examples	Approval Policy
Schema changes	Add column, create index, drop table	Reviewed by DBA and app owner
Data migrations	Populate column from legacy value, update rows conditionally	Reviewed + testable
Seed data	Insert roles, config records, lookup values	Stored per environment; approved once
Patches/hotfixes	Targeted updates to fix data corruption	Reviewed; require rollback script

Environment-Specific Behavior

Each environment receives changes independently. No automatic promotion is allowed across environments.

Env	Behavior
Dev	Runs all new migrations automatically for fast feedback
Test/UAT	Requires merge and promotion trigger
Stage	Pre-prod staging with optional review
Prod	Requires final approval + pipeline controls (e.g., downtime windows, change ticket, rollback script available)

For prod environments, we:

- Require migration prechecks (row count, locks)
- Optionally simulate the migration in a cloned production snapshot
- Enforce rollback readiness

Rollback and Disaster Recovery

Every approved schema change must have a defined rollback strategy. This can include:

- Reverse SQL scripts (/db/rollback)
- Liquibase rollback commands
- Restore from backup (automated snapshot before deploy)
- Conditional scripts (idempotent with environment variables)

Rollback plans are included in the deployment metadata and linked to the change ticket. In the event of a rollback, the same pipeline handles reversion, with an approval gate.

Test Integration and Data Validation

To ensure changes are non-breaking and safe:

- Migrations are tested on ephemeral DB instances during CI (Docker or scratch RDS)
- Integration and functional tests run against the post-migration schema
- Data integrity checks (record counts, value ranges) are executed where applicable
- Synthetic transactions or health checks validate that the application continues to function

We enforce DB test coverage for:

- New constraints
- Triggers
- Non-null column changes
- Downstream foreign key relationships

Access Controls and Credentials

Vendors **do not receive direct access to any live or test databases**. They interact through:

- Git commits
- PR reviews
- CI/CD triggers

Credential handling:

- DB creds are stored in secure secret managers.
- CI/CD deploys pull credentials at runtime.
- Least-privilege DB roles are used per environment (read-only, read-write, admin).
- Passwords are rotated regularly and never embedded in scripts or code.

Compliance, Audit, and Governance

Every change is tied to:

- A JIRA or change request ticket
- A Git commit ID
- A PR with review history
- A pipeline execution record

Audit logs include:

- Who authored the migration
- Who approved it
- Which environments it was applied to
- What data or schema objects it touches
- Whether rollback was available or invoked

These records feed into compliance dashboards and are retained per internal data retention policy.

Security, Compliance, and Audit Logging

Access Health CT's modernization initiative must prioritize security, regulatory compliance, and audit traceability from the ground up. With multiple vendors contributing across environments, it is imperative that the platform enforces **non-negotiable security policies**, implements **fine-grained access control**, and provides **end-to-end visibility** into who changed what, when, where, and how.

This section outlines the security architecture and compliance model that governs infrastructure, application delivery, source control, and access to the environment. The focus is on **zero-trust principles, policy-as-code, secure defaults**, and **continuous auditability**, enabling secure collaboration without compromise.

Security Objectives

The overarching goals of Access Health CT's platform security strategy include:

- Centralized control of all user, system, and vendor access across environments
- Environment-level and role-based isolation for every user and integration
- Continuous policy enforcement through automation
- Full traceability and auditability of every access, change, deployment, and login
- Alignment with regulatory frameworks (e.g., CMS MARS-E, HIPAA, NIST 800-53)

Identity and Access Management (IAM)

Centralized Identity

All access to infrastructure, code, CI/CD platforms, observability systems, and management consoles is federated through Access Health CT's central identity provider (e.g., Azure AD, Okta, or equivalent).

- **SSO is required** for all internal and external users
- External vendors are onboarded using **identity federation** or **limited-scope identities** with expiration policies
- MFA is enforced for all access across cloud consoles, SCM platforms, and bastion hosts

Role-Based Access Control (RBAC)

RBAC is applied across all layers of the stack:

- SCM (e.g., repo read/write/approve)
- CI/CD platforms (e.g., trigger access, deployment rights)
- Cloud infrastructure (e.g., VM shell access, secret vault access)
- Observability tools (e.g., dashboard visibility vs. admin rights)

Each role is scoped by:

- **Environment** (dev, test, prod)
- **Function** (developer, reviewer, deployer, admin)
- **Vendor** (external contributors are scoped to their team domain)

Secure Software Supply Chain

Code and Dependency Scanning

All repositories are scanned automatically on PR and merge:

- **Static Application Security Testing (SAST)**
- **Dependency vulnerability scanning** (SBOM generation, CVE resolution)
- **Secrets scanning** (detecting credentials, tokens, hardcoded keys)

All critical issues block pipeline progression until remediated.

Approved Module Registries

Only **pre-approved, signed artifacts** are allowed in builds:

- Artifacts are pulled from a secure internal registry
- Container images are validated using **image scanning and policy enforcement**
- IaC modules (Terraform, Helm charts, etc.) are version-locked and scanned

Environment and Network Security Controls

Network Segmentation

- Each environment (dev, test, stage, prod) has its **own VPC, subnet, and routing policy**
- Vendor sandboxes are completely isolated
- All external access requires jump hosts or VPNs with audit logging

Firewalls and Ingress Rules

- **Least privilege port and IP access rules** enforced at the subnet and security group level
- Public endpoints are **protected behind WAFs or API gateways**
- Default-deny policies apply to all unscoped traffic

Audit Logging and Traceability

Everything that happens in the system must be observable and attributable through the following audit log domains.

- **Access logs** (SSH, console, UI, DB)
- **Deployment logs** (who deployed what, when, where, and how)
- **Pipeline logs** (build/test/deploy trace)
- **Source control logs** (PR submitter, reviewers, merge metadata)
- **Secrets access logs** (who accessed what, and why)

Vendor Access Security Lifecycle

Phase	Action
Onboarding	Role scoped, time-boxed, access recorded, NDA/compliance training
Active Engagement	Access logging, secret scoping, activity monitoring
Offboarding	Immediate credential revocation, audit log review, auto-triggered secret rotation

Vendor Model

The success of Access Health CT's modernization initiative relies not only on platform design but also on **how external vendors are onboarded, integrated, and governed** throughout the lifecycle of their engagement. In the new model, vendors no longer operate independently with siloed processes or unmanaged environments. Instead, they are **onboarded into a centrally controlled, preconfigured platform** where their access, contributions, and interactions are explicitly defined and continuously monitored.

This section defines the **vendor engagement lifecycle**, detailing each phase from onboarding to offboarding, as well as the tooling and automation that support it. It ensures that **every vendor operates within guardrails**, collaborates through secure workflows, and is accountable for their actions through built-in traceability.

This section outlines exactly how vendors will interact with the platform — from onboarding to offboarding — within the secure, automated, and auditable boundaries established in earlier sections.

The vendor lifecycle under the modern delivery model consists of the following stages:

1. Pre-Engagement Setup
2. Formal Onboarding
3. Access Provisioning
4. Environment Allocation
5. Code Contribution and Delivery
6. Collaboration and Communication
7. Monitoring and Reporting
8. Offboarding and Closure

Each stage is supported by automation, documentation, and platform controls to ensure a consistent, secure, and compliant experience.

Pre-Engagement Setup

Prior to onboarding, internal stakeholders prepare the vendor engagement through the following steps:

- Define the **scope of work** in the form of technical charters or JIRA epics
- Assign a **technical sponsor** from Access Health CT (typically a Product Owner or Platform Engineer)
- Create initial **repository structure** (application, infra, data) if not exist
- Register the vendor in the **central identity management system**
- Define the **access profile**: systems, environments, tools, and expiration

This stage ensures there is a documented contract for **what the vendor will do, where they will work, and how their output will be integrated.**

Formal Onboarding

Once approved, vendors go through a structured onboarding process:

- **Kickoff Session**: Led by DevOps and Application teams; covers platform structure, policies, and expectations
- **Compliance Check**: Vendor signs NDA, Acceptable Use Policy, and completes any required CMS/HIPAA compliance training
- **Tool Orientation**: Vendors are introduced to:
    - Source code structure
    - CI/CD pipeline interfaces
    - Test environments
    - Deployment rules
    - Logging and monitoring dashboards
- **Credentials Issued**: Vendor is provisioned with access tokens, SSO credentials, and assigned permissions (e.g., GitHub repo contributor role)

All onboarding steps are tracked through a ticketing system (e.g., ServiceNow, JIRA) and verified by the internal onboarding checklist.

Access Provisioning

Access is **delegated by role, time, and environment**. Typical vendor roles include:

- Contributor (Code + Documentation)
- Reviewer (if dual delivery)
- Pipeline trigger (deployment, test execution)
- Read-only observer (dashboards, logs)

Access is provisioned using identity federation and RBAC. Access policies:

- Are **scoped per environment** (e.g., dev only)
- Are **time-bound** (e.g., project duration, renewed monthly/quarterly)
- Require **MFA and SSO**
- Are **fully auditable**

Access violations (e.g., access outside hours, unauthorized resource touch) trigger alerts and are logged.

Environment Allocation

Depending on the scope, vendors may be allocated:

- Shared **integration environments** (e.g., test, QA, UAT)
- **Isolated sandboxes** for individual development and testing
- **Short-lived preview environments**, spun up via pipeline for each PR or branch

Environment setup includes:

- Preloaded service dependencies
- Preconfigured secrets and configs
- Access to approved data (anonymized/test-safe)
- Automatic teardown policy for ephemeral envs (e.g., after 72 hours)

Each environment is tagged with the vendor ID, owning team, and expiration metadata.

Code Contribution and Delivery Workflow

Once environments and access are ready, vendors follow a **strict but flexible contribution process**:

1. **Fork or branch** from internal SCM repository (dev, feature/vendor-id/issue)
2. **Develop locally or in a sandbox**; use internal IDE images or pre-configured runners if required
3. **Push code and open PR**; complete required metadata fields (JIRA ID, risk level, testing notes)
4. **Run CI pipeline** automatically on PR:
    - Linting
    - Security scans
    - Unit tests
    - Change validation (e.g., DB plan step)
5. **Undergo review by Access Health CT reviewers**
6. **Merge and trigger deploy**, if approved, to dev/test/UAT

Production deployments always require internal approval, gated promotion, and pre- and post-validation.

Collaboration and Communication Channels

All communications are conducted through **pre-approved channels** for accountability and audit:

- **Slack/MS Teams channels** per vendor/project
- **JIRA Service Desk** for support or triage
- **Documentation repos** for proposals, architecture discussions
- **Office hours or sprint reviews** to align weekly delivery expectations

Vendors are expected to maintain transparency, provide deployment notes, and surface blockers proactively.

Monitoring and Reporting Expectations

Access Health CT provides vendors with **read-only access** to the following:

- **Build and pipeline logs** for their services
- **Application-level monitoring dashboards**
- **Error reporting and alerts**, scoped by application namespace
- **Cost dashboards** (if sandbox envs are metered)

Vendors are expected to:

- Monitor logs after each deploy
- Validate CI build quality regularly
- Respond to incident pings or automated alerts
- Submit weekly status summaries or delivery metrics

Offboarding and Engagement Closure

At the conclusion of a vendor engagement (or personnel turnover), the following workflow is triggered:

1. **Access review** ticket created and assigned to the IAM team
2. **Revoke credentials**: SSO, vault secrets, repo permissions, cloud roles
3. **Teardown environments** associated with the vendor (sandbox, preview)
4. **Archive or lock contributions** if required
5. **Trigger secrets rotation** if the vendor had elevated access
6. **Final audit review** to validate log completeness and change handover

The offboarding process is treated with the same rigor as onboarding and is mandatory for all vendors.

Conclusion

Access Health CT's modernization strategy represents more than a technology upgrade — it is a fundamental shift in how we architect, deliver, and govern digital systems that support the health and well-being of the residents we serve.

Through this document, we have laid out a **platform-first, automation-driven, security-conscious model** that balances the need for internal control with the flexibility to support a multi-vendor ecosystem. By standardizing infrastructure provisioning, enforcing structured CI/CD pipelines, centralizing source code ownership, and embedding security and observability into every layer, we create a resilient foundation for future application delivery — regardless of who builds or maintains the software.

APPENDIX B

REQUIREMENTS TRACEABILITY MATRIX

APPENDIX B: Requirements Traceability Matrix

The Requirements Traceability Matrix (RTM) is a Microsoft Excel file that is located at: https://agency.accesshealthct.com/solicitations. The file consists of several sheets, and each sheet features several columns with blank, fillable cells. With the exception of the first sheet, titled "Categories," the Exchange's business requirements (each requirement, a "Business Requirement") can be found in each sheet's first, second, and third columns. The fourth and fifth columns in each sheet are titled "Compliance" and "Comments," respectively. Respondents must review and answer all "Compliance" and "Comments" cells in each sheet for each Business Requirement in accordance with the below instructions. **Respondents must then submit a completed RTM, in a PDF format, as part of their Proposal.**

RTM Instructions

1. If a Respondent *expects to meet a Business Requirement* as written, the Respondent should enter "MTR" in the corresponding "Compliance" cell. ("MTR" stands for "MEETS THE REQUIREMENT" and indicates that the Respondent can meet the Business Requirement as written.)

If the Respondent *does not agree to comply* with a Business Requirement as written, or has some proposed modification(s) to the requirement language, the Respondent should do one (1) of the following:

a. If the Respondent **does not agree to comply with** the Business Requirement – The Respondent should enter "DNC" in the corresponding "Compliance" cell. ("DNC" stands for "DOES NOT COMPLY OR UNABLE TO DELIVER CAPABILITY" and indicates that the Respondent does not agree or will not be able to comply with the requirement as written.)

b. If the Respondent has some **minor modification** to the Business Requirement – The Respondent should enter "RMM" in the corresponding "Compliance" cell. ("RMM" stands for "REQUIRES MINOR MODIFICATION" and indicates that the Respondent has to implement minor modifications to comply with the requirement as written.)

c. If the Respondent has some **significant modification** to the Business Requirement – The Respondent should enter "RSM" in the corresponding "Compliance" cell. ("RSM" stands for requires "REQUIRES SIGNIFICANT MODIFICATION" and indicates that the Respondent has to implement significant modifications to comply with the requirement as written.)

2. A Respondent who enters "RMM" or "RSM" in a "Compliance" cell must perform the following:

First, the Respondent must copy and paste the corresponding Business Requirement as written from the "Business Requirement" cell into the corresponding "Comments" cell.

Second, the Respondent should strike (using red font) the original text (if necessary) and/or add proposed new text in blue font to clearly indicate any proposed minor or major modification(s) to the original text.

Third, AFTER completing the proposed revision(s), the Respondent must add a concise explanation of the reason for the proposed minor or major revision. The explanation should be separate and distinct from the marked-up text.

3. Respondents may separately use the "Comments" column to provide optional commentary to any Business Requirement.

NOTE: A Respondent should not view the possibility of requesting changes as an opportunity to rewrite the Business Requirements. The Exchange expects a Respondent to comply with the Business Requirements as written. It is generally expected that a Respondent should make changes only for minor clarifications or if the Respondent will not comply with a Business Requirement as written. Major changes must be accompanied by an explanation of how the proposed change would provide improvements in quality, cost and overall effectiveness.

The Exchange will assume that any Business Requirement that a Respondent fails to respond to cannot be met by the Respondent.

APPENDIX C

INDEPENDENT CONTRACTOR AGREEMENT

INDEPENDENT CONTRACTOR AGREEMENT

THIS INDEPENDENT CONTRACTOR AGREEMENT (this "Agreement") is entered into as of _____ (the "Effective Date"), by and between the **Connecticut Health Insurance Exchange d/b/a Access Health CT**, a quasi-public agency created by the State of Connecticut (the "State") pursuant to Public Act 11-53, with an office at 280 Trumbull Street, 15th Floor, Hartford, Connecticut 06103 (the "Exchange"), and _____ , a_____ [corporation, partnership, etc.] with an office at _____ (the "Contractor").

WHEREAS, the Exchange requires a new integrated eligibility and enrollment platform;

WHEREAS, the Exchange issued a Request for Proposals for a Health Insurance Exchange Integrated Eligibility and Enrollment Platform on September 23, 2025 (the "RFP");

WHEREAS, the Contractor submitted a proposal in response to the RFP (the "RFP Response") and the Exchange selected the Contractor to perform the Services (defined below) described in the RFP and further detailed in this Agreement; and

WHEREAS, the Exchange wishes to engage the Contractor to perform the Services subject to the terms and conditions set forth in this Agreement.

NOW, **THEREFORE**, the parties agree as follows:

1. Scope of Services. The Contractor shall perform the Services specified in Exhibit A (the "Services"), in accordance with its RFP Response (incorporated into this Agreement as Appendix B).
2. Administration.
    a. The individuals in charge of administering this Agreement on behalf of the Exchange and the Contractor, respectively, are set forth in Exhibit A.
    b. If the Exchange requests that a staff member of the Contractor no longer provide Services to the Exchange under this Agreement, the Contractor shall remove such staff member from the assignment within seven (7) days. Upon the request of the Exchange, the Contractor shall augment the remaining staff with staff acceptable to the Exchange.
3. Time of Performance and Term.
    a. The Contractor shall perform the Services at such times and in such sequence as may be reasonably requested by the Exchange. The Contractor shall comply with any timeline or deadlines set forth in Exhibit A.
    b. Except as otherwise set forth in Exhibit A, this Agreement will run from its Effective Date until the completion of the Services to the reasonable satisfaction of the Exchange, unless sooner terminated as provided in Section 4.
4. Termination.
    a. Notwithstanding any other provision of this Agreement, the Exchange may terminate this Agreement at any time for any reason. The Exchange shall notify the Contractor in writing,

specifying the effective date of the termination and the extent to which the Contractor must complete performance of the Services prior to such date.

b. Upon receipt of written notification of termination from the Exchange, the Contractor shall immediately cease to perform the Services (unless otherwise directed by the Exchange in the notice) and provide the Exchange with a final invoice for Services performed as of the effective date of termination. Upon written request from the Exchange, the Contractor shall assemble and deliver to the Exchange all Records (as defined in Section 8(a) below), in its possession, custody or control; except for one copy being retained to keep record of obligations subject to the confidentiality obligations set forth in Section 14.

c. Within forty-five (45) days of final billing, the Exchange shall pay the Contractor for Services completed to the reasonable satisfaction of the Exchange and for any out-of-pocket costs to which the Contractor is entitled pursuant to Exhibit A. Notwithstanding any other term of this Agreement, the Contractor shall not be entitled to receive, and the Exchange shall not be obligated to tender to the Contractor, any payments for anticipated or lost profits.

5. Payment.

a. The Exchange shall compensate the Contractor as set forth in Exhibit A.

b. The Exchange will compensate Contractor for the Services only after the submission of itemized documentation, in a form acceptable to the Exchange. Unless otherwise specified in Exhibit A, the Contractor shall bill the Exchange monthly with payment due no sooner than thirty (30) days from the receipt of the invoice. The Exchange may require the Contractor to submit such additional accounting and information as it deems to be necessary or appropriate, prior to authorizing payment under this Section. The Exchange will make payment(s) to Contractor via an electronic funds transfer (ACH) to Contractor's financial institution, which must be a domestic institution or a state or federally licensed foreign bank branch.

c. Invoices submitted late by the Contractor may result in delayed payment.

d. The Exchange shall reimburse the Contractor for those out-of-pocket disbursements and expenses (at cost), as are detailed in Exhibit A, or as otherwise approved in writing in advance by the Exchange. The Exchange shall not reimburse the Contractor for any overhead-related expenses, including, but not limited to, duplicating, secretarial, facsimile (other than long-distance telephone line charges), clerical staff, proofreading staff, meals and in-state transportation costs.

e. The Exchange may set off any costs or expenses that it incurs because of Contractor's unexcused non-performance under this Agreement against those undisputed amounts that are due or may become due from the Exchange to the Contractor under this Agreement, or any other agreement that the Contractor has with the Exchange. This right of setoff will not be deemed to be the Exchange's exclusive remedy for the Contractor's breach of this Agreement. The Exchange reserves the right to exercise any, and all other remedies available to it, all such remedies to survive any setoffs.

6. Cross Default.

a. If the Contractor breaches, defaults or in any way fails to perform satisfactorily under this Agreement, then the Exchange may treat any such event as a breach, default or failure to perform under any other agreements or arrangements ("Other Agreements") that the Contractor has with the Exchange. Accordingly, the Exchange may then exercise any, and all of

its rights or remedies provided for in this Agreement or Other Agreements, either selectively or collectively and without such election prejudicing any other rights or remedies of the Exchange, as if the Contractor had breached the Other Agreements.

b. If the Contractor breaches, defaults or in any way fails to perform satisfactorily under any Other Agreements with the Exchange, then the Exchange may, without any action whatsoever required of the Exchange, treat any such event as a breach, default or failure to perform under this Agreement. Accordingly, the Exchange may then exercise any, and all of its rights or remedies provided for in the Other Agreements or this Agreement, either selectively or collectively and without such election prejudicing any other rights or remedies of the Exchange, as if the Contractor had breached this Agreement.

7. Representations and Warranties. The Contractor represents and warrants to the Exchange for itself and for the Contractor Agents (as defined herein), as applicable, that:

   a. The Contractor and Contractor Agents possess the experience, expertise and qualifications necessary to perform the Services;

   b. The Contractor and where applicable, the Contractor Agents, duly and validly exist under the laws of their states of organization and possess authorization to conduct business in the State of Connecticut in the manner contemplated by this Agreement. The Contractor has taken all necessary action to authorize the execution, delivery and performance of this Agreement and has the power and authority to execute, deliver and perform its obligations under this Agreement;

   c. The execution, delivery and performance of this Agreement will not violate, be in conflict with, result in a breach of or constitute (with or without due notice and/or lapse of time) a default under any of the following, as applicable: (1) any provision of law; (2) any order of any court or the state; or (3) any agreement, document or other instrument to which the Contractor is a party or by which it may be bound;

   d. Neither the Contractor nor any Contractor Agent is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from transactions with any governmental entity;

   e. Neither the Contractor nor any Contractor Agent has been convicted of, or had a civil judgment rendered against them, for commission of fraud or a criminal offense in connection with obtaining or performing a transaction or contract with any governmental entity;

   f. Neither the Contractor nor any Contractor Agent is presently indicted or, to the best of the Contractor's knowledge, under investigation for, or otherwise criminally or civilly charged by, any governmental entity with commission of any of the offenses listed above;

   g. None of the Contractor's prior contracts with any governmental entity have been terminated by the governmental entity for cause; and

   h. The Contractor will not use Contractor Agents to perform the Services who are not employees of the Contractor without the Exchange's prior written consent. Upon receipt of such consent and prior to the performance of the Services by such Contractor Agent, the Contractor shall secure an assignment to the Exchange of any Work Product (as defined in Section 8 (c)) produced by such Contractor Agent.

8. Records/Intellectual Property.

a. The term “Records” means all working papers and such other information and materials Contractor or Contractor Agents accumulate or generate in performing under this Agreement, including, but not limited to, Work Product, artifacts, documents, source data, code, source code output, execute decks, presentations, plans, books, computations, drawings, specifications, notes, reports, records, estimates, summaries and correspondence, kept or stored in any form, including by magnetic or electronic means.

b. Contractor shall provide the Exchange with a copy of all artifacts, documents, reports, source code, source code output, execute decks, presentations and any other Records that may be requested on a quarterly basis for back up purposes. The Contractor, upon written request from the Exchange, shall promptly give to the Exchange, all original Records, or, in the sole discretion of the Exchange, copies thereof. The Contractor shall otherwise maintain all original Records, or copies thereof, for a period of ten (10) years after the termination of this Agreement.

c. The term “Work Product” means every task and deliverable set forth in Exhibit A, milestone, invention, modification, discovery, design, development, customization, configuration, improvement, process, software (excluding pre-existing intellectual property of Contractor, Contractor Agents, subcontractors or third parties), work of authorship, documentation, formula, datum, code technique, know how, secret, or intellectual property whatsoever or any interest therein (whether patentable or not patentable or registerable under copyright or similar statues or subject to analogous protection) that is made, conceived, discovered, or reduced to practice by Contractor or Contractor Agents or subcontractors (either alone or with others) on behalf of the Exchange pursuant to this Agreement.

d. The Exchange shall own all Records resulting from the Services rendered by Contractor or the Contractor Agents under this Agreement and no one else shall have any right, including, but not limited to, any copyright, trademark, or other intellectual property rights in those Records. Contractor shall ensure the Contractor Agents assign to the Exchange any rights they have in the Work Product. All Work Product is a “work made for hire” under U.S. Copyright law and owned solely by the Exchange. In the event and to the extent the Work Product or any portion thereof is deemed for any reason not to be a “work made for hire,” Contractor agrees to and does hereby assign to the Exchange all right, title and interest to such Work Product.

e. The Contractor represents and warrants that the Services and all Work Product resulting from the Services (except the accurate reproduction of information or materials supplied by the Exchange) will not infringe any third-party copyright, patent, trademark, trade secret or other proprietary right. Notwithstanding anything set forth in this Agreement, Contractor shall not use any third-party materials or pre-existing material, including without limitation, open source software or software owned by or licensed to the Contractor, in the Services or any Work Product resulting from the Services, without the Exchange’s prior written consent; provided that upon receipt of such consent, the Contractor shall secure for the Exchange an assignment or perpetual non-cancellable sublicense from such third party to use such software or materials as agreed to by the Exchange, or such materials shall not be used to provide the Services.

f. Neither party will gain by this Agreement any rights of ownership of copyrights, patents, trade secrets, trademarks or any other intellectual property rights owned by the other.

9. Insurance.

a. Before commencing performance of the Services, the Contractor shall obtain and maintain at its own cost and expense for the duration of this Agreement, the following insurance:

i. Commercial General Liability: Contractor shall maintain commercial general liability coverage in the minimum amount of One Million Dollars ($1,000,000) combined single limit per occurrence for bodily injury, personal injury and property damage, and an annual aggregate of Five Million Dollars ($5,000,000). Coverage shall include Premises and Operations, Independent Contractors, Contractual Liability and Broad Form Property Damage coverage.

ii. Automobile Liability: Contractor shall maintain automobile coverage in the amount of Five Hundred Thousand Dollars ($500,000) combined single limit per accident for bodily injury. Coverage extends to owned, hired and non-owned automobiles. If the Contractor does not own an automobile, but one is used in the performance of the Services, then only hired and non-owned coverage is required.

iii. Workers' Compensation and Employer's Liability: Contractor shall maintain coverage in compliance with applicable workers' compensation laws. Coverage shall include Employer's Liability with minimum limits of One Hundred Thousand Dollars ($100,000) each accident, Five Hundred Thousand Dollars ($500,000) Disease - Policy Limit, and One Hundred Thousand Dollars ($100,000) Disease - each employee.

iv. Professional Liability: Contractor shall maintain Errors and Omissions coverage in a form acceptable to the Exchange in the minimum amount of Twenty Million Dollars ($20,000,000) per claim and an annual aggregate of Twenty Million Dollars ($20,000,000).

v. Network Liability: Contractor shall maintain Network Liability coverage with a minimum limit of liability of not less than Twenty Million Dollars ($20,000,000) per claim and an annual aggregate Twenty Million Dollars ($20,000,000) in effect upon the execution of this Agreement. This policy shall have coverages for network interruption; privacy liability inclusive of personal information in any format; security breaches from a network event; and damages from unauthorized breaches into customer and employee information. It shall also provide for forensic expenses, legal expenses, public relations/crisis management and credit monitoring.

b. Contractor must name the Exchange and the State of Connecticut as additional insureds on the Commercial General Liability policy described in Section 9(a) and such policy must be endorsed accordingly. Coverage required under this Agreement shall be primary over any insurance or self-insurance program carried by the Exchange or the State. The insurance policies required hereunder must include provisions: (i) stating that each carrier will waive all rights of recovery, under subrogation or otherwise, against the Exchange, the State and their respective officers, agents, employees, and volunteers; and (ii) preventing cancellation or non-renewal without at least 45 days (10 days for nonpayment of premium) prior notice.

c. Contractor shall provide certificates evidencing the insurance coverage required by this Agreement to the Exchange upon execution of this Agreement. No later than 15 days prior to the expiration date of any such coverage, the Contractor shall deliver to the Exchange certificates of insurance evidencing renewals thereof.

10. Indemnification.

a. The Contractor shall indemnify, defend, and hold harmless the Exchange, the State and their respective officers, directors, representatives, agents, employees, successors, and assigns from and against any and all Claims (as defined below), liabilities, damages, losses, costs and expenses, including but not limited to reasonable attorneys' fees and other professionals' fees, arising, directly or indirectly, in connection with Claims, Acts, or the Agreement and resulting from (a) misconduct or negligent or wrongful acts (whether of commission or omission) of the Contractor or any of the Contractors Agents under the supervision or control of the Contractor while rendering professional services under this Agreement, or (b) any breach or non-performance by the Contractor of any representation, warranty, duty, or obligation of the Contractor under the Agreement ((a) and (b) each and collectively, the "Acts"). The term "Claims" means all actions, suits, claims, demands, investigations and proceedings of any kind, pending or threatened, whether mature, unmatured, contingent, known or unknown, at law or in equity, in any form, including without limitation any third party infringement claims; claims arising out of the acts or omissions of the Contractor's Agents and claims arising out of a breach of the Contractor's representations and warranties.

b. The term "Contractor Agents" means the Contractor's members, directors, officers, shareholders, partners, managers, representatives, agents, servants, consultants, employees, or any other person or entity whom the Contractor retains to perform under this Agreement in any capacity.

11. Independent Contractor. The Contractor is an independent contractor of the Exchange. This Agreement will not create the relationship of employer and employee, a partnership or a joint venture between the Contractor and the Exchange. The Contractor is solely liable for all wages, benefits and tax withholding for itself and shall comply with all applicable tax laws. Neither party is an agent of the other nor will either party have any authority to bind the other.

12. Compliance with Laws. The Contractor and Contractor Agents shall comply with all applicable state and federal laws and municipal ordinances in satisfying obligations under this Agreement, including, but not limited to, Connecticut General Statutes Title 1, Chapter 10, concerning the State's Codes of Ethics. In any event, the Contractor shall be liable for the acts or omissions of the Contractor Agents.

a. The Contractor shall comply, to the extent applicable, with the requirements of Connecticut General Statutes § 4-61dd pertaining to a "large state contractor", as defined in subsection (k) of

Connecticut General Statutes § 4-61dd. Pursuant to Connecticut General Statutes § 4-61dd(h), if an officer, employee or appointing authority of the Contractor takes or threatens to take any personnel action against any employee of the Contractor in retaliation for such employee's disclosure of information to any employee of the Exchange or the Auditors of Public Accounts or the Attorney General under the provisions of subsection (a) or subdivision (1) of subsection (e) of Connecticut General Statutes § 4-61dd, the Contractor shall be liable for a civil penalty of not more than five thousand dollars for each offense, up to a maximum of twenty per cent of the value of the Agreement. Each violation shall be a separate and distinct offense and in the case of a continuing violation each calendar day's continuance of the violation shall be deemed to be a separate and distinct offense. The executive head of the Exchange may request the Attorney General to bring a civil action in the superior court for the judicial district of Hartford to seek imposition and recovery of such civil penalty.

13. Notice of Special Compliance Requirements. The Contractor shall comply with all provisions set forth on Exhibit B with respect to Nondiscrimination and Affirmative Action, Certain State Ethics Requirements, and Applicable Executive Orders.

14. Confidentiality.

a. In the event and to the extent that the Contractor or its Contractor Agents have access to information which is confidential or of a proprietary nature to the Exchange, including, but not limited to, Records, enrollment lists and personal data and personally identifiable information, technical, marketing and product information and any other proprietary and trade secret information, whether oral, graphic, written, electronic, or in machine readable form ("Confidential Information"), the Contractor agrees, for itself and its Contractor Agents, to keep all Confidential Information strictly confidential and not to use or disclose to others the Confidential Information without the Exchange's prior written consent. The Contractor and its Contractor Agents shall comply with all applicable laws regarding personally identifiable information, including without limitation, the privacy and security standards and obligations adopted in accordance with 45 C.F.R. § 155.260(b)(3), and those privacy and security standards and obligations are hereby incorporated into this Agreement by reference. If the Contractor or its Contractor Agent is required to disclose Confidential Information by law or order of a court, administrative agency, or other governmental body, then it shall provide the Exchange with prompt notice of the order or requirement, so that the Exchange may seek a protective order or otherwise prevent or restrict such disclosure.

b. With respect to the Contractor's obligations to maintain the privacy and security of personally identifiable information:

    i. The Contractor shall monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls;

    ii. The Contractor shall promptly inform the Exchange of any change in its administrative, technical or operational environments that would require an alteration of the standards of this Agreement; and

    iii. The Contractor shall bind any subcontractor to the same privacy and security standards and obligations to which the Contractor has agreed in this Agreement.

c. If applicable, Contractor shall develop and document access agreements for Contractor's organizational information systems, consistent with the provisions of the Affordable Care Act and the requirements of 45 CFR §155.260 – Privacy and security of personally identifiable information, paragraphs (b)(2) and (c). Contractor shall review and update the access agreements as part of the system security authorization or when an applicable contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first. Contractor shall ensure that individuals requiring access to organizational information and information systems: (1) Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and (2) Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated.

d. If applicable, Contractor shall develop and document personnel security requirements including security roles and responsibilities for third-party providers, which:

    i. Requires third-party providers to comply with personnel security policies and procedures established by the Contractor; and

    ii. Requires third-party providers to notify Contractor of any personnel transfers or terminations of third-party personnel who possess Contractor credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.

    Contractor shall monitor third-party provider compliance with the requirements set forth in this subsection, as applicable.

e. If applicable, Contractor shall develop and document requirements for the use of external information systems that will:

    i. For Contractor Agents and non-Contractor Agents (such as business partners), prohibit the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process Confidential Information, unless explicitly authorized, in writing, by Contractor. If external information systems are authorized, the Contractor shall establish strict terms and conditions for their use, and in the case of non-Contractor Parties, such terms and conditions must be approved in advance by the Exchange prior to the granting of such authorization. The terms and conditions must address, at a minimum:

        1. The types of applications that can be accessed from external information systems;
        2. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
        3. How other users of the external information system will be prevented from accessing federal information;
        4. The use of VPN and stateful inspection firewall technologies;
        5. The use of and protection against the vulnerabilities of wireless technologies;

6. The maintenance of adequate physical security controls;
7. The use of virus and spyware protection software; and
8. How often the security capabilities of installed software are to be updated.

ii. If Contractor desires to authorize the use of external information systems by non-Contractor Agents, the Exchange must consent to such authorization and the terms and conditions governing use must be approved in advance by the Exchange prior to Contractor's authorization of such use by a non-Contractor Agent. Following approval by the Exchange, the terms and conditions will allow authorized Non-Contractor Agents to:

1. Access the information system from external information systems; and
2. Process, store, or transmit Contractor-controlled information using external information systems.

f. If applicable, Contractor shall develop and document terms and conditions for the use of non-Contractor owned information systems, system components, or devices to process, store, or transmit Confidential Information. Use of Contractor-owned devices must: (i) be documented within the Agreement and Contractor's system security plan, (ii) employ information security and privacy protections appropriate for the sensitivity of the data, and (iii) be approved by the Exchange in advance. Use of personally owned devices must comply with Contractor's policies and directives on use of personally owned information systems and components.

g. The Contractor acknowledges that the Exchange is subject to the Connecticut Freedom of Information Act ("FOIA"). As a result, information provided to the Exchange by the Contractor or any Contractor Agent, regardless of its form, may not be considered confidential, even if marked as such. In no event shall the Exchange have any liability for the disclosure of documents or information in its possession, which the Exchange believes it is required to disclose pursuant to FOIA or any other law. For any information that Contractor believes to be exempt from disclosure under FOIA, Contractor must identify the specific information, provide enough explanation and rationale to justify each claimed exemption consistent with Connecticut General Statutes § 1-210(b) and provide a redacted version of the document to the Exchange. For the avoidance of doubt, Contractor cannot claim a general exemption from FOIA for the entirety of any document.

15. Background Checks.
    a. Contractor shall ensure that each individual who will provide Services under this Agreement has passed the following background checks and screenings:

        i. A Statewide check in the individual's state of residence, a statewide or county check for any other states of residence (depending upon availability);

        ii. A Federal check;

        iii. A Nationwide check;

        iv. Social security trace and validation checks;

v. Citizenship and validation of each individual's eligibility to legally work in the United States; and

vi. FBI fingerprinting (Completion of FD-258).

b. Contractor shall not allow any individual who has been convicted of (i) any felony or (ii) a misdemeanor involving dishonesty, breach of trust, or money laundering to perform any Services for the Exchange, except where prohibited by local or state law.

16. Notices. Any notice required or permitted to be given under this Agreement shall be deemed to be given when hand delivered or one (1) business day after pickup by any recognized overnight delivery service. All such notices shall be in writing and shall be addressed as follows:

If to the Exchange:

Connecticut Health Insurance Exchange d/b/a Access Health CT
280 Trumbull Street, 15th Floor
Hartford, CT 06103
Attention: Director of Legal and Governmental Affairs

If to the Contractor:

17. Miscellaneous.

a. This Agreement will be governed and construed in accordance with the laws of the State of Connecticut, without regard to its conflicts of law principles. The parties irrevocably consent to the exclusive jurisdiction and venue of any state or federal court of competent jurisdiction in Hartford County, Connecticut in any action, suit, or other proceeding arising out of or relating to this Agreement and waive any objection to venue based on the grounds of *forum non conveniens* or otherwise.

b. This Agreement will be binding upon and inure to the benefit of the parties and their respective successors and permitted assigns. Notwithstanding the foregoing, the Contractor may not assign this Agreement or delegate its duties without the Exchange's prior written permission. Any assignment in violation of this provision will be null and void. The Exchange may transfer or assign its rights and obligations under this Agreement without the prior written consent of the Contractor. This Agreement will not be binding on the Exchange, and the Exchange will assume no liability for payment for Services, unless and until a copy of the Agreement, executed on behalf of each party, is delivered by the Exchange to the Contractor.

c. If any provision of this Agreement, or application to any party or circumstances, is held invalid by any court of competent jurisdiction, the balance of the provisions of this Agreement, or their application to any party or circumstances, will not be affected, provided that neither party would then be deprived of its substantial benefits hereunder.

d. The Exchange and the Contractor shall not be excused from their respective obligations to perform in accordance with this Agreement, except in the case of force majeure events and as

otherwise provided for in this Agreement. In the case of any such exception, the nonperforming party shall give immediate written notice to the other, explaining the cause and probable duration of any such nonperformance. "Force majeure events" means events that materially affect the time schedule within which to perform and are outside the reasonable control of the party asserting that such an event has occurred, including, but not limited to, labor troubles unrelated to the Contractor, failure of or inadequate permanent power, unavoidable casualties, fire not caused by the Contractor, extraordinary weather conditions, disasters, riots, acts of God, insurrection or war.

e. The Contractor shall not refer to the Services provided to the Exchange hereunder for the Contractor's own advertising or promotional purposes, including, but not limited to, posting any material or data on the Internet, without the Exchange's prior written approval.

f. The Contractor shall cooperate with any, and all, audits or review of billing by the Exchange or any other agency, person or entity acting on behalf of the Exchange, and shall provide billing in a format, which will facilitate audit or review.

g. The Contractor shall continue to perform its obligations under this Agreement while any dispute concerning this Agreement is being resolved, unless otherwise instructed by the Exchange in writing.

h. Neither the failure nor the delay of any party to exercise any right under this Agreement on one or more occasions will constitute or be deemed a waiver of such breach or right. Waivers will only be effective if they are in writing and signed by the party against whom the waiver or consent is to be enforced. No waiver given by any party under this Agreement will be construed as a continuing waiver of such provision or of any other or subsequent breach of or failure to comply with any provision of this Agreement.

i. Nothing in this Agreement will be construed as a modification, compromise or waiver by the Exchange of any rights or defenses or any immunities provided by federal or state law to the Exchange or any of its officers and employees. To the extent that this Section conflicts with any other section, this Section will govern.

j. The captions in this Agreement are inserted only as a matter of convenience and for reference and in no way define, limit or describe the scope of this Agreement or the scope of content of any of its provisions.

k. Any provision of this Agreement, the performance of which requires that it be in effect after the expiration and/or termination of this Agreement, will survive such expiration and/or termination, including without limitation, any assignment, license, confidentiality, warranty and indemnification obligations.

l. This Agreement, including all exhibits and schedules hereto, constitutes the entire agreement between the parties and supersedes all other agreements, promises, representations, and negotiations, regarding the subject matter of this Agreement.

m. No amendment or modification of this Agreement or any of its provisions will be effective unless it is in writing and signed by both parties.

n. This Agreement may be executed in any number of counterparts and by electronic, facsimile or e-mailed signature. All such counterparts taken together will, for all purposes, constitute one agreement binding upon all parties to this Agreement.

IN WITNESS WHEREOF, the duly authorized representative of each party has read and signed this Agreement.

CONNECTICUT HEALTH INSURANCE EXCHANGE d/b/a ACCESS HEALTH CT	**[CONTRACTOR]**
_____	_____
[NAME]	**[NAME]**
[TITLE]	**[TITLE]**

Exhibit A

Services

The Contractor shall perform the following services under this Agreement (the "Services"):

Staffing

The staff members of the Contractor primarily responsible for the performance of this Agreement are _____. The Contractor may not change these individuals without the prior written consent of the Exchange, which consent will not be unreasonably withheld.

Administration

The individual in charge of administering this Agreement on behalf of the Exchange is _____.

The individual in charge of administering this Agreement on behalf of the Contractor is _____.

Deadlines/Timeline

Contractor shall perform the Services in a timely manner consistent with the needs of the Exchange, recognizing that the Exchange will require immediate assistance. If not sooner terminated in accordance with the provisions of this Agreement, the term of this Agreement shall expire on _____, 20___.

Compensation

[Insert RFP Response Compensation Details.]

The Contractor shall be compensated solely for work performed, documented and accepted by the Exchange. The maximum total amount that the Contractor may be paid under this Agreement shall not exceed _____ Dollars ($_____).

Billing

The Contractor shall submit invoices to the Exchange on a monthly basis in accordance with any invoice submission instructions provided by the Exchange. Invoices shall, at a minimum, include the Contractor name, purchase order number and/or contract number (if applicable), the billing period, the dates worked, the number of hours worked each day (billed to the tenth of an hour within a single workday) with a brief synopsis of the work performed, the rate being charged for the Contractor, and the total cost for the Contractor's work during the billing period.

Exhibit B

A. Nondiscrimination and Affirmative Action

a) For purposes of this Section A of this Exhibit B, the following terms are defined as follows:

i. "Commission" means the Commission on Human Rights and Opportunities;
ii. "Contract" and "contract" include any extension or modification of this Agreement;
iii. "Contractor" and "contractor" means _____ and includes any successors or assigns of the Contractor or contractor;
iv. "Gender identity or expression" means a person's gender-related identity, appearance or behavior, whether or not that gender-related identity, appearance or behavior is different from that traditionally associated with the person's physiology or assigned sex at birth, which gender-related identity can be shown by providing evidence including, but not limited to, medical history, care or treatment of the gender-related identity, consistent and uniform assertion of the gender-related identity or any other evidence that the gender-related identity is sincerely held, part of a person's core identity or not being asserted for an improper purpose;
v. "good faith" means that degree of diligence which a reasonable person would exercise in the performance of legal duties and obligations;
vi. "good faith efforts" shall include, but not be limited to, those reasonable initial efforts necessary to comply with statutory or regulatory requirements and additional or substituted efforts when it is determined that such initial efforts will not be sufficient to comply with such requirements;
vii. "marital status" means being single, married, widowed, separated or divorced as recognized by the State of Connecticut (the "State");
viii. "mental disability" means one or more mental disorders, as defined in the most recent edition of the American Psychiatric Association's "Diagnostic and Statistical Manual of Mental Disorders," or a record of or regarding a person as having one or more such disorders;
ix. "minority business enterprise" means any small contractor or supplier of materials fifty-one percent or more of the capital stock, if any, or assets of which are owned by a person or persons: (1) who are active in the daily affairs of the enterprise, (2) who have the power to direct the management and policies of the enterprise, and (3) who are members of a minority, as such term is defined in subsection (a) of Connecticut General Statutes § 32-9n; and
x. "public works contract" means any agreement between any individual, firm or corporation and the State or any political subdivision of the State other than a municipality for construction, rehabilitation, conversion, extension, demolition or repair of a public building, highway or other changes or improvements in real property, or which is financed in whole or in part by the State, including, but not limited to, matching expenditures, grants, loans, insurance or guarantees.

For purposes of this Section, the terms "Contract" and "contract" do not include an agreement where each contractor is (1) a political subdivision of the state, including, but not limited to, a municipality, (2) a quasi-public agency, as defined in Connecticut General Statutes § 1-120, (3) any other state, including but not limited to, any federally recognized Indian tribal governments, as defined in Connecticut General Statutes § 1-267, (4) the federal government, (5) a foreign

government, or (6) an agency of a subdivision, agency, state or government described in the immediately preceding enumerated items (1), (2), (3), (4) or (5).

b) (1) The Contractor agrees and warrants that in the performance of the Contract such Contractor will not discriminate or permit discrimination against any person or group of persons on the grounds of race, color, religious creed, age, marital status, national origin, ancestry, sex, sexual orientation, gender identity or expression, status as a veteran, status as a victim of domestic violence, intellectual disability, mental disability or physical disability, including, but not limited to, blindness, unless it is shown by such Contractor that such disability prevents performance of the work involved, in any manner prohibited by the laws of the United States or of the State of Connecticut; and the Contractor further agrees to take affirmative action to ensure that applicants with job-related qualifications are employed and that employees are treated when employed without regard to their race, color, religious creed, age, marital status, national origin, ancestry, sex, sexual orientation, gender identity or expression, status as a veteran, status as a victim of domestic violence, intellectual disability, mental disability or physical disability, including, but not limited to, blindness, unless it is shown by the Contractor that such disability prevents performance of the work involved; (2) the Contractor agrees, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, to state that it is an "affirmative action equal opportunity employer" in accordance with regulations adopted by the Commission; (3) the Contractor agrees to provide each labor union or representative of workers with which the Contractor has a collective bargaining agreement or other contract or understanding and each vendor with which the Contractor has a contract or understanding, a notice to be provided by the Commission, advising the labor union or workers' representative of the Contractor's commitments under this section and to post copies of the notice in conspicuous places available to employees and applicants for employment; (4) the Contractor agrees to comply with each provision of this Section and Connecticut General Statutes §§ 46a-68e and 46a-68f and with each regulation or relevant order issued by said Commission pursuant to Connecticut General Statutes §§ 46a-56, 46a-68e and 46a-68f; and (5) the Contractor agrees to provide the Commission on Human Rights and Opportunities with such information requested by the Commission, and permit access to pertinent books, records and accounts, concerning the employment practices and procedures of the Contractor as relate to the provisions of this Section and Connecticut General Statutes § 46a-56. If the contract is a public works contract, the Contractor agrees and warrants that it will make good faith efforts to employ minority business enterprises as subcontractors and suppliers of materials on such public works projects.

c) Determination of the Contractor's good faith efforts shall include, but shall not be limited to, the following factors: The Contractor's employment and subcontracting policies, patterns and practices; affirmative advertising, recruitment and training; technical assistance activities and such other reasonable activities or efforts as the Commission may prescribe that are designed to ensure the participation of minority business enterprises in public works projects.

d) The Contractor shall develop and maintain adequate documentation, in a manner prescribed by the Commission, of its good faith efforts.

e) The Contractor shall include the provisions of subsection (b) of this Section in every subcontract or purchase order entered into in order to fulfill any obligation of a contract with the State and/or the Exchange and such provisions shall be binding on a subcontractor, vendor or manufacturer unless exempted by regulations or orders of the Commission. The Contractor

shall take such action with respect to any such subcontract or purchase order the Commission may direct as a means of enforcing such provisions including sanctions for noncompliance in accordance with Connecticut General Statutes § 46a-56; provided that if such Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the Commission regarding a state contract, the Contractor may request the State of Connecticut to enter into any such litigation or negotiation prior thereto to protect the interests of the State and the State may so enter.

f) The Contractor agrees to comply with the regulations referred to in this Section as they exist on the date of this Contract and as they may be adopted or amended from time to time during the term of this Contract and any amendments thereto.

B. Certain State Ethics Requirements

a) For all State contracts as defined in P.A. 07-01 having a value in a calendar year of $50,000 or more or a combination or series of such agreements or contracts having a value of $100,000 or more, the authorized signatory to this Agreement expressly acknowledges receipt of the State Elections Enforcement Commission's notice advising state contractors of state campaign contributions and solicitation prohibitions and will inform its principals of the contents of the notice.

C. Applicable Executive Orders of the Governor

The Contractor shall comply, to the extent applicable, with the provisions of Executive Order No. Three of Governor Thomas J. Meskill, promulgated June 16, 1971, concerning labor employment practices, Executive Order No. Seventeen of Governor Thomas J. Meskill, promulgated February 15, 1973, concerning the listing of employment openings, and Executive Order No. Sixteen of Governor John G. Rowland, promulgated August 4, 1999, concerning violence in the workplace. These Executive Orders are incorporated into and are made a part of this Agreement as if they had been fully set forth in it. At the Contractor's request, the Exchange shall provide a copy of these orders to the Contractor.

D. IRS Tax Information Security Provisions

I. PERFORMANCE

In performance of this Agreement, the Contractor agrees to comply with and assume responsibility for compliance by its officers or employees with the following requirements:

(1) All work will be performed under the supervision of the Contractor or the Contractor's responsible employees.

(2) The Contractor and Contractor's officers or employees to be authorized access to Federal Tax Information ("FTI") must meet background check requirements defined in Internal Revenue Service ("IRS") Publication 1075. The Contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the Exchange and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this Agreement. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Agreement. Inspection or disclosure of FTI to anyone other than the Contractor or the Contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The Contractor will certify that FTI processed during the performance of this Agreement will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the Exchange. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the Exchange with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this Agreement will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this Agreement apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the Exchange under this Agreement assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the Exchange under this Agreement.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Agreement apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the Contractor is bound and obligated to the Exchange under this Agreement.

(12) For purposes of this Agreement, the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The Exchange will have the right to void the Agreement if the Contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of the Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of the Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of the Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(4) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(5) Granting the Contractor access to FTI must be preceded by certifying that each officer or employee understands the Exchange's security policy and procedures for safeguarding FTI. The Contractor and each officer or employee must maintain their authorization to

access FTI through annual recertification of their understanding of the Exchange's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the Exchange's files for review. As part of the certification and at least annually afterwards, the Contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431. The training on the Exchange's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the Contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Exchange, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Agreement for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

Appendix A

Required Ethics and Nondiscrimination Certifications

Execution of CTHIX Ethics Form 1: Campaign Contribution Certification.
Included in RFP Response, attached as Appendix B.

Gifts, C.G.S. § 4-252: Large State Contract Representation for Contractor.
Pursuant to section 4-252 of the Connecticut General Statutes and Acting Governor Susan Bysiewicz Executive Order No. 21-2, promulgated July 1, 2021, the Contractor, for itself and on behalf of all of its principals or key personnel who submitted a bid or proposal, represents:

(1) That no gifts were made by (A) the Contractor, (B) any principals and key personnel of the Contractor, who participate substantially in preparing bids, proposals or negotiating Exchange contracts, or (C) any agent of the Contractor or principals and key personnel, who participates substantially in preparing bids, proposals or negotiating Exchange contracts, to (i) any public official or employee of the Exchange soliciting bids or proposals for Exchange contracts, who participates substantially in the preparation of bid solicitations or requests for proposals for Exchange contracts or the negotiation or award of Exchange contracts, or (ii) any public official or State employee of any other State agency, who has supervisory or appointing authority over such State agency or quasi-public agency;

(2) That no such principals and key personnel of the Contractor, or agent of the Contractor or of such principals and key personnel, knows of any action by the Contractor to circumvent such prohibition on gifts by providing for any other principals and key personnel, official, employee or agent of the Contractor to provide a gift to any such public official or State employee; and

(3) That the Contractor is submitting bids or proposals without fraud or collusion with any person.

Large State Contract Representation for Official or Employee of the Exchange.
Pursuant to section 4-252 of the Connecticut General Statutes and Acting Governor Susan Bysiewicz Executive Order No. 21-2, promulgated July 1, 2021, the Exchange official represents that the selection of the person, firm or corporation was not the result of collusion, the giving of a gift or the promise of a gift, compensation, fraud or inappropriate influence from any person.

Iran Energy Investment Certification.
(a) Pursuant to section 4-252a of the Connecticut General Statutes, the Contractor certifies that it has not made a direct investment of twenty million dollars or more in the energy sector of Iran on or after October 1, 2013, as described in Section 202 of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010, and has not increased or renewed such investment on or after said date.
(b) If the Contractor makes a good faith effort to determine whether it has made an investment described in subsection (a) of this section shall not be deemed to be in breach of the contract or in violation of section 4-252a of the Connecticut General Statutes. A "good faith effort" for purposes of this subsection includes a determination that the Contractor is not on the list of persons who engage in certain investment activities in Iran created by the Department of General Services of the State of California pursuant to Division 2, Chapter 2.7 of the California Public Contract Code. Nothing in this subsection shall be construed to impair the ability of the State agency or quasi-public agency to pursue a breach of contract action for any violation of the provisions of the Contract.

Consulting Agreements Representation.

Pursuant to section 4a-81 of the Connecticut General Statutes, the Contractor represents that it has not entered into any consulting agreements in connection with this Contract, except for the agreements listed below. "Consulting agreement" means any written or oral agreement to retain the services, for a fee, of a consultant for the purposes of (A) providing counsel to a contractor, vendor, consultant or other entity seeking to conduct, or conducting, business with the State, (B) contacting, whether in writing or orally, any executive, judicial, or administrative office of the State, including any department, institution, bureau, board, commission, authority, official or employee for the purpose of solicitation, dispute resolution, introduction, requests for information, or (C) any other similar activity related to such contracts. "Consulting agreement" does not include any agreements entered into with a consultant who is registered under the provisions of chapter 10 of the Connecticut General Statutes as of the date such contract is executed in accordance with the provisions of section 4a-81 of the Connecticut General Statutes.

_____ _____

Consultant's Name and Title Name of Firm (if applicable)

_____ _____ _____

Start Date End Date Cost

The basic terms of the consulting agreement are: _____

_____

_____

Description of Services Provided: _____

_____

_____

Is the consultant a former State employee or former public official? ☐ YES ☐ NO

If YES:_____ _____

Name of Former State Agency Termination Date of Employment

The undersigned, being the person signing the Contract, swears that the representation in the Consulting Agreements Representation provision in this Contract is made to the best of my knowledge and belief, and is subject to the penalty of false statement as provided in section 53a-157b of the Connecticut General Statutes.

_____

Signature of person signing this Contract

_____

Print Name

Date: _____

Sworn and subscribed before me on this _____ day of _____, 20___.

_____

Commissioner of the Superior Court
or Notary Public

_____
My Commission Expires

Campaign Contribution Restriction.
For all State contracts, defined in section 9-612 of the Connecticut General Statutes as having a value in a calendar year of $50,000 or more, or a combination or series of such agreements or contracts having a value of $100,000 or more, the authorized signatory to this Contract represents that they have received the State Elections Enforcement Commission's notice advising state contractors of state campaign contribution and solicitation prohibitions, and will inform its principals of the contents of the notice. The notice is available here:
https://seec.ct.gov/Portal/data/forms/ContrForms/seec_form_11_notice_only.pdf.

Nondiscrimination Certification.
Pursuant to subsection (c) of section 4a-60 and subsection (b) of section 4a-60a of the Connecticut General Statutes (set forth in **Exhibit B** hereto), the Contractor, for itself and its authorized signatory of this Contract, affirms that it understands the obligations of this section and that it will maintain a policy for the duration of the Contract to assure that the Contract will be performed in compliance with the nondiscrimination requirements of such sections. The Contractor and its authorized signatory of this Contract demonstrate their understanding of this obligation by (A) having provided an affirmative response in the required online bid or response to a proposal question which asks if the contractor understands its obligations under such sections, (B) signing this Contract, or (C) initialing this nondiscrimination affirmation in the following box: ☐

Appendix B

RFP Response

APPENDIX D

ETHICS FORM 1: GIFT AND CAMPAIGN CONTRIBUTION CERTIFICATION

CTHIX Form 1

STATE OF CONNECTICUT
CAMPAIGN CONTRIBUTION CERTIFICATION

Written or electronic certification to accompany a bid or proposal or a non-competitive contract with a value of $50,000 or more, pursuant to C.G.S. § 9-612.

INSTRUCTIONS:

Complete all sections of the form. Attach additional pages, if necessary, to provide full disclosure about any campaign contributions made to campaigns of candidates for statewide public office or the General Assembly, as described herein. Sign and date the form, under oath, in the presence of a Commissioner of the Superior Court or Notary Public. Submit the completed form to the awarding State agency at the time of submission of your bid or proposal (if no bid or proposal– submit this completed form with the earliest submittal of any document to the state or quasi-public agency prior to the execution of the contract), and if there is a change in the information contained in the most recently filed certification, such person shall submit an updated certification either (i) not later than thirty (30) days after the effective date of such change or (ii) upon the submittal of any new bid or proposal for a contract, whichever is earlier.

Check One:

☐ **Initial Certification**

☐ **Updated Certification because of change of information contained in the most recently filed certification**

CAMPAIGN CONTRIBUTION CERTIFICATION:

I certify that neither the contractor or prospective state contractor, nor any of its principals, have made any contributions to, or solicited any contributions on behalf of, any party committee, exploratory committee, candidate for state-wide office or for the General Assembly, or political committee authorized to make contributions to or expenditures to or for, the benefit of such candidates, in the previous four years, that were determined by the State Elections Enforcement Commission to be in violation of subparagraph (A) or (B) of subdivision (2) of subsection (f) of Section 9-612 of the General Statutes, without mitigating circumstances having been found to exist concerning such violation. Each such certification shall be sworn as true to the best knowledge and belief of the person signing the certification, subject to the penalties of false statement. If there is any change in the information contained in the most recently filed certification, such person shall submit an updated certification not later than thirty days after the effective date of any such change or upon the submittal of any new bid or proposal for a state contract, whichever is earlier.

All Campaign Contributions on behalf of any party committee, exploratory committee, candidate for state-wide office or for the General Assembly, or political committee authorized to make contributions to or expenditures to or for, the benefit of such candidate, for a period of four years prior to signing the contract or date of the response to the bid, whichever is longer, include:

Contribution Date	Name of Contributor	Recipient	Value	Description

Sworn as true to the best of my knowledge and belief, subject to the penalties of false statement.

Printed Contractor Name

Printed Name of Authorized Official

Signature of Authorized Official

Subscribed and acknowledged before me this __ day of _____, 20__.

Commissioner of the Superior Court (or Notary Public)

My Commission Expires: