V5.3

CITY OF PHILADELPHIA

Board of Pensions

REQUEST FOR INFORMATION

FOR

Pensions System Modernization

May 20, 2026

Information Session	June 3, 2026, at 10:30am (Local Philadelphia Time) Teams link
Deadline for questions, requests for clarification, or requests for additional information	June 9, 2026, before 5:00pm (Local Philadelphia Time)
City Responds to Questions	June 18, 2026
Responses to RFI Due	June 29, 2026, before 5:00pm (Local Philadelphia Time)

CHERELLE L. PARKER, Mayor
Francis Bielli, Executive Director, Board of Pensions

TABLE OF CONTENTS

Pensions System Modernization RFI
REQUEST FOR INFORMATION

I. RESPONSE CALENDAR

Post Request for Information	May 20, 2026
Information Session	June 3, 2026, at 10:30am (Local Philadelphia Time) Teams link
Deadline for questions, requests for clarification, or requests for additional information (email pensionsmodernization@phila.gov)	June 9, 2026, before 5:00pm (Local Philadelphia Time)
City Responds to Questions https://www.phila.gov/rfp/additional opportunities)	June 18, 2026
Responses to RFI Due (email pensionsmodernization@phila.gov)	June 29, 2026, before 5:00pm (Local Philadelphia Time)

These dates are estimates only and the City reserves the right, in its sole discretion, to alter this schedule as it deems necessary or appropriate. Notice of changes will be posted on the City's website at https://www.phila.gov/rfp/additional opportunities.

II. PURPOSE OF REQUEST FOR INFORMATION

About Philadelphia Pension Board:

Philadelphia Pension Board (Referred to as 'The Board' here onwards) is a public sector retirement system for administering retirement benefits for approximately 35,000 retirees and 29,000 Active employees, 14 Pension plans, and various benefit and contribution rate structures. Through its legacy platform, the board manages retirement benefits for four employers including City of Philadelphia, Philadelphia Parking Authority, Philadelphia Municipal Authority, and Philadelphia Housing and Development Corporation.

The Board is embarking on a significant initiative to modernize its administrative business processes and related legacy technology systems that currently support its business operations. As part of this initiative, the board intends to implement a new Enterprise-wide Pensions Administration System (PHLCers) and Retiree Health and Welfare System. We are looking for information from qualified Pension Administration System (PAS) and Retiree Health and Welfare Systems vendors. We want to understand how your solutions can replace our current legacy system, which is a monolithic pension administration system, along with various miscellaneous

business support applications. For upstream and downstream impact, our Active employee Human Resources (HR) system is Oracle HR and Finance system is a legacy Mainframe and will transition to Workday.

In addition to Pension DB, DC, and Hybrid plans, the City also manages Retiree Health Benefits (medical, Rx, dental, vision, life/AD&D, and others) for eligible members and survivors of Self-insured, fully insured, Non-represented and union supported, and Medicare-supported plans. Respondents should include capabilities for administering retiree health benefits, including enrollment, re-enrollments, co-pays and contributions management, Waives, Age-outs, deferrals, Medicare reimbursements, opt-outs, and integration with third-party health plan administrators.

The goal of this RFI is to:

- Gain comprehensive understanding of the current market landscape for modern Pension Administrative System solutions.
- Gain comprehensive understanding of the current market landscape of Retiree Health Benefits Administration solutions
- Identify vendors capable of supporting the complex administration of our multi-tiered and multi-employer pension plans.
- Evaluate potential technology architectures, implementation approaches, and ongoing support models.
- Inform the development of a detailed Request for Proposal (RFP).
- Inform pricing expectations for future budget requests.

Respondents are asked to provide the Board with information regarding their available products and solutions according to VI. ANTICIPATED SOLUTION REQUIREMENTS, subject to the following guidelines:

- Identify only COTS products that are modifiable or configurable to meet specific City requirements, and that focus on interoperability, reliability, usability, availability, capacity and scalability
- Present the software solution's interoperability and operational requirements in accordance with the International Organization for Standardization Open Systems Interconnection (OSI) model
- Include an architectural diagram of the solution with a description of the solutions scalability; responses may include one or more models or solutions
- Describe the configurability of the software to meet the specified requirements and services.

Responses should include implementation, integration, and/or configuration services. If, the software can be installed and configured only by the Respondent, that must be clearly stated in the Response, including the reasons why that is the case.

Respondents may, in the City's discretion, be invited to engage in discussions with the City's project team and/or demonstrate their products, services and solutions.

No contract will be awarded pursuant to this RFI. Anyone who does not respond to this RFI is not precluded from responding to any future solicitation issued by the City. The City intends to procure software for this project as soon as reasonably possible, in accordance with the City's procurement laws and practices for software purchases, which may include, but are not limited to, the use of existing City contracts or certified cooperative purchase agreements. Respondents will not be bound by the ROM cost estimates provided in their responses to this RFI in a future procurement. The City also reserves the right to not procure any software.

III. RFI CONTACT INFORMATION FOR QUESTIONS, REQUESTS FOR CLARIFICATION

All questions (see RFI Question Template Exhibit) and requests for clarification concerning this RFI must be in writing and submitted via email no later than 5:00 pm, Local Philadelphia Time, on June 9, 2026, to:

pensionsmodernization@phila.gov

Responses to questions and requests for additional information shall be at the sole discretion of the City. Any additional information and/or responses to questions will be posted only on the City's website at https://www.phila.gov/rfp/additional opportunities . No additional information and/or responses to questions will be sent by email. Nothing in this RFI shall create an obligation on the City to respond to a Respondent submitting a response.

The City may, in its sole discretion, issue addenda to this RFI containing responses to questions, clarifications of the RFI, revisions to the RFI or any other matters that the City deems appropriate. Addenda, if any, will be posted on the City's website at https://www.phila.gov/rfp/additional opportunities. It is the Respondent's responsibility to monitor the Additional Opportunities site for Addenda and to comply with any new information.

Oral responses made by any City employee or agent of the City in response to questions or requests for information or clarification related to this RFI are not binding and shall not in any way be considered as a commitment by the City.

If a Respondent finds any inconsistency or ambiguity in the RFI or an addendum to the RFI issued by the City, the Respondent is requested to notify the City in writing by the above deadline for questions and requests for information or clarification.

IV. ABOUT THE CITY OF PHILADEPHIA

The City of Philadelphia is the largest city in the Commonwealth of Pennsylvania and the sixth-most populous city in the United States with over 1.5 million residents. Additionally, due to its rich historic and cultural heritage, the region is visited by more than 40 million people each year.

Philadelphia is located in the southeastern section of Pennsylvania, and the coterminous city/county covers 143 square miles. The City is bordered by the following counties: Bucks, Montgomery and Delaware in Pennsylvania, and Burlington, Camden and Gloucester in New Jersey.

As an operating department of the City, Board of Pensions provides pension administration and retirement management services to the City, its employees, and City retirees. There are over 25,000 city employees in Philadelphia.

V. INFORMATION SESSION

An Informational Session to review the requirements of this RFI will be held virtually via Microsoft Teams on June 3, 2026, starting at 10:30AM (Local Philadelphia Time).

Meeting link: https://teams.microsoft.com/meet/251392052402998?p=DWWLZ2hyi6t00N4KtP

Attendance at the Information Session is optional but strongly encouraged.

VI. ANTICIPATED SOLUTION REQUIREMENTS

The proposed solution should include the following functionality. The Pension Board is seeking information from vendors regarding their pension administration system solutions. We are looking for partners who can provide innovative solutions that align with our commitment to member service excellence.

Key Capabilities

Please indicate your system's capabilities in the following key areas:

- Pension Administration (Admin) Activities
- Retiree Health Benefits Administration
- Member Portal
- Employer Portal
- Workflow Management
- Document Management
- Member Education & Engagement
- Artificial Intelligence

In addition to the Key Capabilities, please highlight any differentiating features as listed on the following tables.

☐	Admin Activities	Highlight Any Differentiating Features
☐	Maintain and view demographic data	
☐	Maintain and view employment and position data	
☐	Submit wage and contribution data similar to employers	
☐	Maintain and view salary and contribution data	
☐	Maintain and view service credit data	
☐	Maintain and view tier and plan data	
☐	Maintain and view member transactions	
☐	Maintain and view member earnings	
☐	Maintain and view general ledger transactions	
☐	Maintain employer/employee contribution rate components for all plans	
☐	Accept and view benefit applications	
☐	View and generate benefit estimates	
☐	Allow for divorce calculations, divorce reductions, divorce deductions, and alternate payee account creations (QDRO) – Do you have Ocular text ability?	
☐	Allow for pre-retired death calculations (Service connected and ordinary death)	
☐	Allow for ordinary retirement calculations	
☐	Allow for withdrawal calculations	
☐	Allow for post-retirement death calculations	
☐	Allow for member Service Purchase credits for various approved services	
☐	Allow for disability calculations (Service connected and ordinary)	
☐	Retiree/Beneficiary benefit disbursement Payroll processing including Regular, Supplemental, Withdrawal, and lumpsum for DROP (Deferred Retirement Option Plan) payments	
☐	Process taxes and periodic regulatory and tax requirements	
☐	Allow for manual employer and member invoicing	

☐	Allow for manual checks	
☐	Payment for recipients (paper checks and electronic funds transfer, both domestic and international)	
☐	Allow for benefit adjustments (annual and ad-hoc)	
☐	Maintain web accounts for member, employer, and PHIP TPA portals	
☐	View and maintain member and employer billing statements	
☐	View employer statements including side accounts and statement history	
☐	View employer statement details by date range in a filterable, sortable format	
☐	Generate member annual statements extract data (1099R)	
☐	Generate actuarial data extract	
☐	Ability to manage retiree health benefit eligibility, enrollment, and re-enrollment	
☐	Ability to calculate premium and billing for retirees	
☐	Ability to retire Health Benefit coverage for certain number of years	
☐	Ability to track deferrals	
☐	Ability to track Medicare eligibility and status change	
☐	Ability to support multiple health plans and coverage tiers	
☐	Ability to report on compliance with Health Benefits	
☐	Ability to upload regulatory documents including 1095s and 1094s and link to retiree accounts	

☐	Member Portal	Highlight Any Differentiating Features
☐	Verification letters (Retirees and beneficiaries)	
☐	Account information access	
☐	Ability to update specific demographic information	
☐	Access to documents (i.e. member monthly and annual statements, 1099Rs)	
☐	Online transactions and form submission (state type of transactions)	

☐	Offer benefit calculators	
☐	Form submission/claims Status tracking	
☐	Seminar registration and appointment scheduling	
☐	Ability to choose communications preference (online versus paper)	
☐	Secured access (see more information in the security section of this RFI, VI.vi.4.1)	
☐	Ability to configure to our branding standards	
☐	Ability to support all major devices and browsers with responsive ADA compliant UI/UX	
☐	View and update health benefit elections.	
☐	Access health plan documents and coverage details.	
☐	Ability to complete annual enrollment and life events	
☐	Ability to access regulatory documents	
☐	Ability to defer Health and Welfare for certain number of years	
☐	Ability to upload documents securely via the member portal such as marriage certificate	

☐	Employer Portal	Highlight Any Differentiating Features
☐	Ability to create, submit, and maintain records and reports for demographic and wage data	
☐	Ability to review submitted reports	
☐	Ability to review posted records	
☐	Ability to review data for all past, current, and future employees reported to PERS	
☐	Access tasks submitted by PERS for data verification, Leave of Absence, salary certification, salary breakdown, or any other type of data request needed (work item requests)	
☐	Ability to review and export employer statements (financial statements) by plan type, statement period, and fund	

☐	Secured access (see more information in the security section of this RFI, VI.vi.4.1)	
☐	Ability to communicate with PERS via the portal	
☐	Ability to support all major devices and browsers with responsive, ADA compliant UI/UX	

☐	Workflow Management	Highlight Any Differentiating Features
☐	Task assignment and tracking	
☐	Status updates visible to members	
☐	Process automation	
☐	Performance metrics	

☐	Document Management	Highlight Any Differentiating Features
☐	Available system that works with new PAS	
☐	Integration with existing systems	
☐	Electronic forms	
☐	Digital signatures and alternative authentication	

☐	Member Education and Engagement	Highlight Any Differentiating Features
☐	Event scheduling capabilities	
☐	Appointment management	
☐	Virtual meeting support	

☐	Artificial Intelligence	Highlight Any Differentiating Features
☐	Current AI capabilities	
☐	Member service applications	
☐	Administrative efficiency improvements	

i.

VII. SUBMISSION GUIDELINES

The City expects each Respondent to include in their response to this RFI the following items in the order listed:

Company Overview:

Please provide a brief overview of your company:

- Company name, address, and website
- Primary contact person for this RFI (name, title, phone, email)
- Company history and size
- Third party business partners or co-partners
- Primary ownership of core software
- Office locations
- References/Other similar sized organizations where the product/services are implemented
- List any partnerships with other governmental jurisdictions where you have solutions to pensions plans and retiree Health and welfare
- Note the company's operations including the number of years the company has been supporting this solution; location of company's headquarters and all other office locations; and three years of financial data to ensure company stability.

Experience:

Describe your company/organization's relevant experience (and that of partners, when applicable) with modern pensions administration systems. Identify your experience with clients of similar size and scope to the City of Philadelphia, including client name, engagement title, description of engagement, the solution implemented and the methodology used, cost, the start and completion dates of the project, as well as, the name, address and telephone number of a contact person.

Product/Software Solution:

Identify one or more solutions that meet the City's requirements. Responses that describe solutions which are completely custom software may, in the City's discretion, be rejected without review.

A major goal of this RFI is to provide Respondent with an opportunity to inform the City and Board of Pensions about their respective software solution's interoperability and operational requirements in reference to the OSI model. Respondents are encouraged to include in their response an architectural diagram of the solution with description of the solution's scalability. Respondents are welcome to provide one or more models or solution sets to meet this requirement for an integrated interoperable solution set.

Infrastructure/Architecture Model:

Identify the infrastructure/architecture model(s) you provide and support, and whether they are on-premise, hosted off-premise, or Software-as-a-Service (SaaS) models.

Supplement this request with an interoperable architectural diagram outlining each OSI layer requirement for enablement, sustainment, reliability, redundancy, and growth. Highlight your anticipated annual upgrade and patch release schedule.

Key Features:

Identify best of breed features included in the proposed COTS solution(s), including, at a minimum, the Key Features in Section VI. Anticipated Project Requirements.

Support and Maintenance Model:
Provide the anticipated ongoing software maintenance and support services required to sustain the solution including frequency of upgrades and patches/bug releases and the estimated timeframes to complete. Outline the services in your support model including available service level agreements.

Training Model:
Outline the services in your training model for administrative and end user training including the training services, methodology, and typical schedule. Include the pricing model for training services and the methodology and schedule.

Reporting and Key Performance Indicators (KPIs):
Provide the standard and custom reporting included in your solution and the available KPIs. Include information on data input and export capabilities; security and auditing, and dashboards and metrics.

Pricing/Licensing Model:
Include a general pricing model and costs for the software based upon the information provided in this RFI. This pricing should also indicate the licensing model, (i.e. licensing by individual users, by core, by seat etc.), descriptions of the hosting models available, and estimates of associated costs. Include cost estimates for ongoing support and maintenance for three years, and when those support and maintenance costs begin (i.e. at time of purchase, after implementation, etc.). If applicable, include a list of additional items or services/software needed to operate the system that are not included and must be provided/purchased by the City.

Respondents will not be bound by any cost estimates included in responses to this RFI.

VIII. USE OF RESPONSES

Responses to this RFI may be used by the Board to select a software product for the new Pensions system and a new Retiree Health system. Responses may also be used to assist the Board in gathering information for planning purposes, and for purposes of identifying sufficient resources for an implementation initiative.

The City does not intend to announce any further actions taken pursuant to this RFI. If any such announcements are made, at the sole discretion of the City, those announcements will be posted with the original RFI. In some cases, at the City's sole discretion, the City may issue an RFP. The City will notify Respondents to this RFI once the RFP has been posted on the City's website.

The City will notify you if additional information is required in order to evaluate your response to this RFI. Absent such follow up from the City, we respectfully request that respondents refrain

from requesting additional information on the status of this RFI. In order to protect the integrity of the City procurement process, City personnel will not respond to requests for additional information on the status or outcome of this RFI, other than as described above.

IX. HOW TO SUBMIT RESPONSES

Respondents should submit their responses electronically (hard copies are unacceptable) in MS Word or Adobe PDF format, as a single document (see note below), to:

pensionsmodernization@phila.gov

Responses are due June 29, 2026, before 5:00 PM, Local Philadelphia Time.

Note: Response document(s) are limited to 15 MB; if necessary, please submit multiple files or zip/compress the file(s)

X. CONFIDENTIALITY AND PUBLIC DISCLOSURE

Respondents shall treat all information obtained from the City which is not generally available to the public as confidential and/or proprietary to the City. Respondents shall exercise all reasonable precautions to prevent any information derived from such sources from being disclosed to any other person. No other party, including any Respondent, is intended to be granted any rights hereunder.

XI. RIGHTS AND OPTIONS RESERVED

In addition to the rights reserved elsewhere in this RFI, the City reserves and may, in its sole discretion, exercise any or more of the following rights and options with respect to this RFI if the City determines that doing so is in the best interest of the City:

1. Decline to consider any response to this RFI ("response"); cancel the RFI at any time; elect to proceed or not to proceed with discussions or presentations regarding its subject matter with any Respondent and with firms that do not respond to the RFI; to reissue the RFI or to issue a new RFI (with the same, similar or different terms);

2. Select a COTS package from a vendor that does not respond to this RFI, or elect not to proceed with any procurement;

3. Waive, for any response, any defect, deficiency or failure to comply with the RFI if, in the City's sole judgment, such defect is not material to the response;

4. Extend the Submission Date/Time and/or to supplement, amend, substitute or otherwise modify the RFI at any time prior to the Submission Date/Time, by posting notice thereof on the City web page(s) where the RFI is posted;

5. Require, permit or reject amendments (including, without limitation, submitting information omitted), modifications, clarifying information, and/or corrections to responses by some or all Respondents at any time before or after the Submission Date/Time;

6. Require, request or permit, in discussion with any Respondent, any information relating to the subject matter of this RFI that the City deems appropriate, whether it was described in the response to this RFI;

7. Discontinue, at any time determined by the City, discussions with any Respondent or all Respondents regarding the subject matter of this RFI, and/or initiate discussions with any other Respondent or with vendors that did not respond to the RFI;

8. To conduct such investigations with respect to the financial, technical, and other qualifications of the Respondent as the City, in its sole discretion, deems necessary or appropriate;

9. Do any of the foregoing without notice to Respondents or others, except such notice as the City, in its sole discretion, may elect to post on the City web page(s) where this RFI is posted.

This RFI and the process described are proprietary to the City and are for exclusive benefit of the City. Upon submission, responses to this RFI shall become the property of the City, which shall have unrestricted use thereof.

XII. PUBLIC DISCLOSURE

By submitting a response to this RFI, Respondent acknowledges and agrees i) that the City is a "local agency" under and subject to the Pennsylvania Right-to-Know Law (the "Act"), 65 P.S. §§ 67.101-67.3104, as the Act may be amended from time to time; and ii) responses may be subject to public disclosure under the Act. In the event the City receives a request under the Act for information that a Respondent has marked as confidential, the City will use reasonable efforts to consult with Respondent regarding the response and, to the extent reasonably practicable, will give Respondent the opportunity to identify information that Respondent believes to be confidential proprietary information, a trade secret, or otherwise exempt from access under Section 708 of the Act.

Notwithstanding anything to the contrary contained in this RFI, nothing in this RFI shall supersede, modify, or diminish in any respect whatsoever any of the City's rights, obligations, and defenses under the Act, nor will the City be held liable for any disclosure of records, including information that the City determines in its sole discretion is a public record and/or information required to be disclosed under the Act.

XIII. CITY OF PHILADELPHIA SECURITY ADDENDUM

This Security Addendum ("**Addendum**") is attached to, incorporated into, and forms a part of, the master service agreement, statement of work, vendor agreement, purchase order, or other terms (the "**Agreement**") under which the vendor identified in the Agreement (the "**Provider**") provides services to the City of Philadelphia ("**City**") (each a "**Party**" and collectively the "**Parties**"). In the event of any conflict between the terms of this Addendum, any other documents comprising the Agreement, and any Business Associate Agreement ("**City PHI Terms**") and/or Security Addendum by and between the Parties, the conflict will be governed in the following order: (1) the City PHI Terms; (2) this Addendum; (3) the Data Processing Addendum; and (4) the Agreement.

WHEREAS City may provide access to or disclose information, records, documents, and data in relation to the work required under the Agreement, including information about its business, employees, and/or City, as well as Personal Information as that term is defined in the Pennsylvania Breath of Personal Information Notification Act (as amended) (collectively, "**City Data**") for the purpose of receiving the Provider's services under the Agreement; and

All City Data and the systems on which they reside must be protected in accordance with City security and privacy documentation and system risk, to include, at a minimum, adequate safeguards for the following:

Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary City Data;

Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and

Availability, which means ensuring timely and reliable access to and use of City Data.

NOW, THEREFORE, the Parties agree as follows:

1. **FIPS 199.** The Provider's Services and Systems will be categorized by the City and managed by the Provider based on the Federal Information Processing Standard (FIPS) Publication 199 of Low Impact, Moderate Impact, or High Impact.

2. **Security and Privacy Governance.** Provider shall maintain a cybersecurity program that documents the policies, standards, and controls it uses that secure the information and resources related to the Services. The documentation shall include organizational, administrative, technical, and physical safeguards and standards appropriate to the size, complexity, and scope of the activities, and the sensitivity of the City Data at issue.

3. **Artificial Intelligence/Machine Learning Disclosure.** The Provider must disclose if their Services and Systems include embedded Artificial Intelligence (AI) and/or Machine Learning (ML) components. If such technologies are utilized, the Provider shall provide documentation detailing the AI frameworks employed and demonstrate adherence to relevant AI compliance frameworks, such as the EU AI Act, NIST AI Risk Management Framework, ISO/IEC 42001 (AI Management System), or other recognized AI governance standards. The Provider will update relevant compliance documentation as changes occur and provide notice of any such updates to the City.

4. Network Management.

a. **Asset Management.** Provider will perform asset management of all end points, or inventory, supporting directly or indirectly the System and City Data. End points include but are not limited to: (i) servers, (ii) workstations, (iii) printers, (iv) cell phones, (v) VoIP, (vi) AV devices, and (vii) physical security devices such as badge readers and CCTV. The Provider will provide an asset inventory list to the City upon request.

b. **Host System Configuration.** Provider has and will configure host systems according to an industry standard, such as ISO 27001. Systems must be configured to function as required and to prevent unauthorized actions. Provider will provide system configuration documentation to the City upon request.

c. **System Network Monitoring.** Provider must maintain an up-to-date continuous monitoring program performing a systematic approach for ongoing surveillance, analysis, and evaluation of the System's security posture and activities. Provider has and will develop and implement an automated process to review and correlate log alerts and security events regularly for all System components in order to identify anomalies or suspicious activity. The review and correlation of log alerts and security events shall include but is not limited to: (i) all security events; (ii) logs of all critical System components; (iii) all privilege access, and (iv) logs of all servers and System components that perform security functions. Server and System component logs must include, but are not limited to, Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Endpoint Detection & Response (EDR), and authentication servers (e.g., Active Directory domain controllers, RACF). Upon request, the Provider will provide evidence of continuous monitoring activities, including results of the monitoring.

d. **Network Controls.** Provider must ensure that all data and communications networks are secured to ensure the protection of City Data. All Provider Systems must remain up to date to the current release and be actively monitored with patches promptly installed.

e. **Encryption.** Provider will encrypt all City Data in transit, in process, and at rest using an encryption solution that meets, at a minimum, Advanced Encryption Standard-256 (AES-256) and Transport Layer Security (TLS) 1.3, or the most secure encryption algorithm available. Provider shall maintain key management practices to safeguard encryption keys used for data handling.

f. **Remote Access.** Remote access to a network containing City Data or access to City systems will be done via a secure connection with an authentication mechanism approved by the City. All extranet connectivity into the City systems will be through City-approved and authorized secure remote connections. If remote access is provided by the City, the Provider is responsible for implementing logging and monitoring mechanisms to track remote access activities. Provider will furnish the City access to the logs upon request.

g. **Access Control.** Provider will restrict access to City Data to only authorized individuals to ensure that (i) only authorized individuals are permitted access to business applications, systems, networks, and computing devices containing City Data; and (ii) user access is scoped to the least privilege required to complete their assigned duties. Provider will review privileged user access, at a minimum, every three (3) months, and non-privileged users, at a minimum, every six (6) months.

h. **Passwords and Multi-Factor Authentication.** The Provider will adhere to all City Identification and Authentication requirements outlined in the Password Standards at a minimum. Provider personnel will use unique passwords that must remain confidential and will not be shared between Provider's employees, contractors, or third-party users.

All access shall require the Provider to use a multifactor authentication method when accessing City Data and City systems and networks.

i. **Malware Controls.** Provider shall ensure the System is protected with up-to-date anti-malware and endpoint detection and response (EDR) software. At all times during the provision of any Services, Provider will make reasonable efforts to ensure that all Services do not contain malicious software or malware. This includes regular scanning, monitoring, and updating of signatures and definitions to safeguard against emerging threats. The City reserves the right to request evidence of implementation and findings.

j. **Vulnerability & Threat Management.** Provider will ensure a vulnerability management program exists to identify and eliminate vulnerabilities and threats that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). The Provider's program will include, at a minimum, regular vulnerability and compliance scanning, independent penetration testing, and threat intelligence analysis. Upon the Provider's identification of vulnerabilities or threats, the Provider shall promptly implement appropriate measures. This includes but is not limited to: (a) vulnerability remediation; (b) software and firmware updates and patching; and (c) hardware maintenance. The Provider will not utilize software or hardware that is End of Life (EOL) and will implement appropriate security packages to remain in compliance.

k. **Data Backups.** To ensure the ability to restore the availability and access to City Data in a timely manner in the event of a physical or technical incident, Provider will ensure that backups of essential information and software, and in particular any City Data, are performed on a regular basis, according to a defined cycle in accordance with Provider's internal policies and industry best practices, but no less than every 48 hours or as directed by the City in writing. Provider will work with the City to determine the Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Maximum Tolerable Downtime (MTD) for the City's Data and system. The City reserves the right to require more frequent backup frequencies based on the criticality of the City's Data and System. Provider shall establish alternate and/or separate storage sites to ensure availability and accessibility of City Data. Provider shall test the backup process at least quarterly.

l. **Secure Destruction.** Provider will implement methods of destruction that are based on the type of media, including physical, paper-based media; physical, digital media; and electronic, digital data. Provider will securely destroy sensitive information and maintain documentation of such destruction.

m. **Virtualization & Cloud Solutions.** If Provider utilizes a cloud solution, Provider will adhere to the same security principles required by this Addendum and applicable government regulations, laws, or directives, including data protection laws, as used throughout Provider's enterprise.

5. **Testing.** Provider will regularly, and in any event at least annually or as changes occur, test, assess, evaluate, and document its compliance with this Addendum to ensure that the measures identified herein are effective for the security of the processing of City Data. The City reserves the right to require independent assessments for some or all categories of required testing. Upon request by the City, Provider will provide City with all final test plans, results, and working papers.

6. **Physical Security.** Provider will actively manage the physical security controls and ensure all buildings throughout Provider's enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) and store, process, or transmit City Data are physically

protected from unauthorized access. These physical security controls should follow security best practices.

7. **Security Incident.** If Provider has knowledge of any suspected or actual access, destruction, loss, theft, use, modification, or disclosure of City Data that is by an unauthorized party or in violation of the Agreement and/or applicable local, state, or federal law (a "Security Incident" or "Incident"), Provider will report such Security Incident to City immediately, and in any event not later than twenty-four (24) hours upon becoming aware of the Security Incident. Provider will comply with any and all Security Incident provisions of the Agreement, including without limitation with respect to notifying and cooperating with the City, responding to the Security Incident, remediating the Security Incident, and assisting the City in complying with its regulatory obligations provided that, if the Agreement does not specify Provider obligations in the event of a Security Incident, Provider will comply with the following:
    a. Notify the City immediately following discovery, but no later than twenty-four (24) hours, of becoming aware of such Incident. Provider's report shall identify:
        i. the nature of unauthorized access, use, or disclosure;
        ii. the City Data accessed, used, or disclosed;
        iii. the person(s) who accessed, used, disclosed, and/or received protected information (if known);
        iv. what Provider has done or will do to mitigate any deleterious effect of the unauthorized access, use, or disclosure; and
        v. what corrective action Provider has taken or will take to prevent future unauthorized access, use or disclosure.
    b. In the event of a Security Incident, Provider shall keep the City informed regularly of the progress of its investigation and provide updates to any information provided to the City as Provider becomes aware of new or changed information until the uncertainty is resolved.
    c. Provider shall coordinate with the City in its Security Incident response activities including without limitation:
        i. Immediately preserve any potential forensic evidence relating to the Incident, and remedy the Incident as quickly as circumstances permit;
        ii. Promptly (within two (2) business days) designate a contact person to whom the City will direct inquiries, and who will communicate Provider responses to City inquiries;
        iii. As rapidly as circumstances permit, apply appropriate resources to investigate, document, and remedy the Incident, to restore City service(s) as directed by the City, and to undertake other response activities, as appropriate;
        iv. Provide status reports to the City on Incident response activities, either on a daily basis or a frequency approved by the City;
        v. Make all reasonable efforts to assist and cooperate with the City in its Incident response efforts;
        vi. Ensure that knowledgeable Provider staff are available on short notice, if needed, to participate in City-initiated meetings and/or conference calls regarding the Incident; and

vii. Cooperate with the City in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by City.

d. Perform or take any other actions required to comply with applicable law as a result of the occurrence, including by cooperating with the City in providing any notices to the competent regulatory authority and the data subjects that the City deems appropriate.

e. Use best efforts to recreate lost City Data in the manner and on the schedule set by City without charge to City.

f. Provide to City a detailed plan within ten (10) calendar days of the occurrence describing the measures Provider will undertake to prevent a future occurrence.

g. Provider shall retain and preserve City Data in accordance with the City's instruction and requests, including without limitation any retention schedules and/or litigation hold orders provided by the City to Provider, independent of where the City Data is stored.

h. Provider will not inform any third party of a Data Breach without the prior, written consent of Client, unless required by applicable laws, and the City shall conduct all media communications related to such Security Incident, unless in its sole discretion, City directs Provider to do so.

8. Audits.

a. Information Security Audit Reports. The City reserves the right to require Provider to produce to the City, no more than one time per year, a SSAE 18, SOC 2, Type II Report, and a SSAE SOC 1 audit report ("Audit Reports") in accordance with the following requirements: (a) the Audit Reports shall include a 365 day (12-month) testing period; and (b) the Provider shall send the City the Audit Reports no longer than thirty (30) days after they are received by Provider.

b. In addition to the above and any other City audit rights in the Agreement, Provider will, upon ten (10) days' prior written notice, contribute to audits during the term of this Addendum by City or a third party designated by City to confirm Provider's compliance with this Addendum. The City, or its designated third party, shall conduct the audit during normal business hours and without undue disruption to Provider's business operations. Audits shall be limited to once per year, unless: (i) Provider has experienced a Security Incident within the prior twelve (12) months which has impacted City Data; or (ii) as further required by a regulatory authority.

9. Cyber Insurance. Provider will maintain cyber insurance coverage during the term of this Addendum in accordance with the Agreement, provided that, if the Agreement does not specify cyber insurance coverage levels, Provider will maintain coverage in accordance with the following:

a. **Limit of liability**: $2,000,000 per claim/aggregate.
b. **Coverage**: Information security and privacy liability that arise under this contract, including, but not limited to: (i) data while in transit or in the possession of any third parties hired by Contractor (such as data back-up services) to electronic system; (ii) loss of damage to or destruction of electronic data breaches arising from unauthorized access or exceeded access; (iii) malicious code, viruses, worms or malware; (iv) electronic business income and extra expense as a result of the inability to access website due to a

cyber-attack or unauthorized access; or (v) Privacy Notification Extra Expense Coverage (including credit monitoring expense).

c. Cyber Liability Insurance may be written on a claims-made basis provided that any retroactive date applicable to coverage under the policy precedes the Effective Date of the Agreement, and that continuous coverage will be maintained, or an extended discovery period will be purchased for a period of at least two (2) years after expiration or termination of this contract.

d. The City of Philadelphia, its officers, employees, and agents shall be named as additional insureds.

10. **No Offshoring**. Provider and its subcontractors will not transmit, export, download, access, store, or maintain any City Data beyond the borders of the United States without the City's prior, written consent. Provider shall not furnish services, software, or hardware from any company or supplier located or based in a country identified as nation-state cyber actor by the Cybersecurity and Infrastructure Security Agency or any successor agency.

11. **Training**. The Provider is responsible for completing all City required security and privacy awareness training as general users, administrators, and/or role-based training, as appropriate. The Provider will be required to complete training internally for all full-time employees and support contractors who have indirect or direct access to City Data and Systems.

12. **Third-Party Vendor Management**. If Provider uses a third-party vendor for support services including software and hardware to provide services to the City, Provider is responsible for verifying and reporting that the third-party vendor is in compliance with this Addendum. The City reserves the right to pre-approve all third-party vendors prior to usage and to require evidence that the Provider has performed due diligence and due care in safeguarding the City Data and system by enforcing this Addendum. The Provider is responsible for reporting the third-party's compliance with this Addendum at least on an annual basis, or when changes occur.

13. **Data Ownership.** The City requires perpetual and unfettered access to its business data in an open and agreed upon format, and by agreed upon access methods for the duration of the Agreement. The City requires extended System access after expiration or termination of the Agreement to retrieve City Data. A minimum period of 180 days of access for data retrieval after contract expiration is required, though a shorter period may be acceptable if the Provider can facilitate data extraction on the City's behalf. Following data extraction by Provider or upon notice by the City, Provider will immediately destroy any copies of any City Data that remain in its possession as described in Section 3.l, above.

    The City reserves the right to require documentation to aid in reconstructing data objects and relationships. This documentation should include:
    a. A Data Dictionary describing data Attributes, Acceptable Values, Field Types, Data Structures, Primary Keys, Foreign Keys, and any other key information regarding the data.
    b. Data Architecture documents including entity relationship diagrams documenting semantic and logical data relationships.

14. **Definitions.**
    a. Services – Services means the services furnished by the Provider under the Agreement.
    b. System – System means the servers, network devices, software, computers, and other equipment, if any, used by the Provider to furnish Services under the Agreement.

Respondent Name:		
Question Number	**RFI Section #** ***(If applicable)***	**Question(s)**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		