PARTICIPATING ADDENDUM
NASPO ValuePoint COOPERATIVE PURCHASING PROGRAM
Computer Equipment
Administered by the State of Minnesota (hereinafter "Lead State")

MASTER AGREEMENT

Master Agreement No: MNWNC-116 IBM Corporation

(hereinafter "Contractor")

And

City of Philadelphia

(hereinafter "Participating State/Entity")

1. Scope: This addendum allows for purchase of the following Computer Equipment/Services: IBM Servers and related equipment led by the State of Minnesota along with a multi-state sourcing team for use by state agencies and other entities located in the Participating State/Entity that is authorized by that state's statutes to utilize state /entity contracts, and which receives prior written approval of the state's chief procurement official.

   The original solicitation contains the requirements and definitions establishing the following Product Bands allowed on the Master Agreement. The Master Agreement identifies the bands awarded to the Contract Vendor. The configuration limits and restrictions for the Master Agreement are provided with revisions identified by the Participating State in this Participating Addendum.

2. Participation: Use of specific NASPO ValuePoint cooperative contracts by agencies, political subdivisions and other entities (including cooperatives) authorized by an individual state's statutes to use state/entity contracts are subject to the prior approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

3. Order of Precedence:

   1. A Participating Entity's Participating Addendum ("PA"); A Participating Entity's Participating Addendum shall not diminish, change, or impact the rights of the Lead State with regard to the Lead State's contractual relationship with the Contract Vendor under the Terms of Minnesota NASPO ValuePoint Master Agreement

   2. Minnesota NASPO ValuePoint Master Agreement (includes negotiated Terms & Conditions)

   3. The Solicitation including all Addendums; and

   4. Contract Vendor's response to the Solicitation

   These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contract Vendor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to the Master Agreement as an Exhibit or Attachment. No other terms and conditions shall apply, including terms and conditions listed in the Contract Vendor's response to the Solicitation, or terms listed or referenced on the Contract Vendor's website, in the Contract Vendor quotation/sales order or in similar documents subsequently provided by the Contract Vendor. The solicitation language prevails unless a mutually agreed exception has been negotiated.

4. Participating State Modifications or Additions to Master Agreement:

(Other modifications or additions apply only to actions and relationships within the Participating Entity.)

Appendix A: see attached the City's Service, Supply, and Equipment Terms and Conditions

5. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name	Karen A. Schneider
Address	4660 La Jolla Village Drive, Ste. 300, San Diego, CA 92122
Telephone	720-397-5563
Fax	
E-mail	kasch@us.ibm.com

Participating Entity

Name	City of Philadelphia, Procurement Department
Address	1401 JFK Boulevard, MSB 120
Telephone	215-686-4750
Fax	
E-mail	Bid.info@phila.gov

6. Partner Utilization: Each state represented by NASPO ValuePoint participating in this Master Agreement independently have the option of utilizing partners. Only partners approved by this Participating State may be deployed. The Participating State will define the process to add partners. The Contractors partners' participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement. For purposes of clarity, "partners" as used in this section 6 are not considered subcontractors as defined in Appendix A: City of Philadelphia Service, Supply, and Equipment Terms and Conditions.

7. Terms: The Participating State/Entity is agreeing to the terms of the Master Agreement only to the extent the terms are not in conflict with applicable law.

8. Orders: Any Order placed by a Participating Entity or Purchasing Entity for a Product and/or Service available from this Master Agreement shall have the NASPO Master Agreement number on the Purchase order in order to be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the Order agree in writing that another contract or agreement applies to such Order.

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating entity: City of Philadelphia, PA	Contractor: International Business Machines Corporation
By: DocuSigned by: Monique Nesmith-Joyner 31897BB77B8C4BB...	By: DocuSigned by: 57D8F4927D58417...
Name: Monique Nesmith-Joyner	Name: KA Schneider
Title: Procurement Commissioner	Title: NASPO Program Manager
Date: July 29, 2020	Date: July 28, 2020
Approved as to Form DocuSigned by: Phillip Bullard D53E7FF627014D0...	
Name: Phillip Bullard	
Title: Senior Attorney	

For questions on executing a participating addendum, please contact:

NASPO ValuePoint

Cooperative Development Coordinator	Tim Hay
Telephone	503-428-5705
E-mail	thay@naspovaluepoint.org

[Please email fully executed PDF copy of this document to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases]

CITY OF PHILADELPHIA
SS&E TERMS AND CONDITIONS OF CONTRACT

1. INDEMNIFICATION.

Contractor's indemnity and limitation of liability obligations shall be as set forth in Attachment A to these Terms and Conditions.

2. DEFAULT and TERMINATION.

The City shall notify Contractor in writing of such termination, which shall be effective as of the date specified in the notice of termination (the "Termination Date"). The Procurement Commissioner may, in his/her sole discretion, require Contractor to continue to furnish all goods and perform all services required under the Contract until the Termination Date, in which case, subject to the remedies enumerated above, the contractor shall be paid in accordance with the Contract therefore. If the City requires Contractor to cure the event(s) of default, or to continue to furnish goods or services until the Termination Date, and Contractor refuses or fails to do so after having been provided a reasonable opportunity to cure, then such failure shall itself be deemed an event of default under this Section, for which the City may exercise any of its rights hereunder.

TAX MATTERS

3. TAX EXEMPTION.

The City of Philadelphia is exempt from the payment of any federal excise or transportation taxes and any Pennsylvania sales tax. The contract must be net, exclusive of taxes. The City will not pay any sales taxes imposed on the contractor. The contractor must not include any sales taxes imposed on the contractor in its costs to be reimbursed by the City. However, when under established trade practice any federal excise tax is included in list prices, contractor may quote the list price and shall show separately the amount of the federal tax, either as a flat sum or as a percentage of the list price, which shall be deducted by the City. In the event contractor pays any sales or use tax, contractor hereby assigns to City, or City's agent, all of its rights, title and interest in any sales or use tax which may be refunded as a result of the purchase of any articles furnished in connection with the Contract and contractor, unless directed by the City, shall not file a claim for any sales or use tax refund subject to this assignment. Contractor authorizes the City, in City's name or the name of contractor, to file a claim for refund of any sales or use tax subject to this assignment.

TAX INDEBTEDNESS.

The City of Philadelphia does not wish to do business with tax delinquents or other businesses indebted to the City. In furtherance of this policy. In furtherance of this policy, the following certifications have been developed and shall form a part of any contract result from the Participating Addendum:

a. Contractor's Certification of Non-Indebtedness. Contractor hereby certifies and represents that to the best of their knowledge and belief, Contractor and Contractor's parent company(ies) and subsidiary(ies) are not currently indebted to the City of Philadelphia (the "City").

4. TAX REQUIREMENTS.

Any person or entity that is awarded a contract by the City and/or School District of Philadelphia, is subject to Philadelphia's business tax ordinances and regulations.

a. The City Solicitor has determined that anyone who is awarded a contract by the City and/or School District pursuant to a bid has entered into a contract within the City, and the subsequent delivery of goods into the City or performance of services within the City constitutes doing business in the City and subjects the contractor, including but not limited to, one or more of the following taxes:

   i. Business Income and Receipts Tax

   ii. Net Profits Tax

   iii. City Wage Tax

   The contractor, if not already paying the aforesaid taxes, is required to apply to the Department of Revenue, 1401 John F. Kennedy Blvd., Public Service Concourse, Municipal Services Building, Philadelphia, PA 19102 for a tax identification number and to file appropriate business tax returns as provided by law. Questions should be directed to the Business and Earnings Tax Unit at (215) 686-6600.

5. Orders Against Contract. Subsequent to contract conformance, purchase orders will be issued at such time that the product and/or service is needed. Such purchase orders will show if delivery is to be made upon receipt of order, or only after notification by the using department.

a. Invoices shall be submitted after delivery and acceptance of the product or service by the City. Payment is due 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later After 45 days, Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Delays can occur because of incomplete or inaccurate invoicing information. To ensure timely payment invoices must include the following:

(1) The Contractor must submit three (3) copies of the invoice for payment to the receiving department listed on the purchase order after the delivery or service has been completed.

(2) The invoice must correctly reference the purchase order number, the vendor name, address and Federal Employer Identification number.

(3) Checks will only be made payable to the company name as shown on the purchase order; the invoice must reflect this same company name as the "pay to".

(4) The invoice must show the quantity and type of item or service and the price.

(5) The unit of purchase on the invoice must agree with the unit cited on the purchase order. Reference to the specific line item is helpful

GENERAL INFORMATION

6. COMPLIANCE WITH LAWS.

The Contractor, in performance of the Contract shall comply with, and all goods, services, documents and other materials furnished under the Contract shall conform with, all applicable federal, state or local laws, ordinances, executive orders, rules, regulations and all court orders, injunctions, decrees and other official interpretations thereof of any federal, state or local court, administrative agency or governmental body, including the City, the Commonwealth of Pennsylvania and the United States of America ("applicable law").

7. NONDISCRIMINATION.

a. Any Contract awarded pursuant to the contract is entered into under the terms of the Philadelphia Home Rule Charter and in its performance, Contractor shall not discriminate nor permit discrimination against any person because of race, color, religion, ancestry, national origin, sex, gender identity, sexual orientation, age or disability. Such discrimination shall constitute an event of default under this Contract entitling City to terminate this Contract forthwith. This right of termination shall be in addition to any other rights or remedies as provided herein or otherwise available to the City at law or in equity.

b. In accordance with Chapter 17-400 of The Philadelphia Code, Contractor agrees that its payment or reimbursement of membership fees or other expenses associated with participation by its employees in an exclusionary private organization, insofar as such participation confers an employment advantage or constitutes or results in discrimination with regard to hiring, tenure of employment. promotions, terms, privileges or conditions of employment, on the basis of race, color, sex, sexual orientation, gender identity, religion, national origin or ancestry, shall constitute an event of default under this Contract and shall entitle the City to all rights and remedies as provided herein or otherwise available to the City at law or in equity. Contractor agrees to include the immediately preceding sentence, with appropriate adjustments for the identity of the parties, in all subcontracts which are entered into pursuant to this Contract. Contractor further agrees to cooperate with the Commission on Human Relations of the City of Philadelphia in any manner which the said Commission deems reasonable and necessary for the Commission to carry out its responsibilities under Chapter 17-400 of The Philadelphia Code. Failure to so cooperate shall constitute an event of default under this Contract entitling the City to all rights and remedies as provided herein or otherwise available to the City at law or in equity.

8. ETHICS REQUIREMENTS.

To preserve the integrity of City employees and maintain public confidence in the competitive bidding system, the City intends to vigorously enforce the various ethics laws as they relate to City employees in the bidding and execution of City contracts. Such laws are in three categories:

a. Gifts. Executive Order No. 10-16 prohibits City employees from soliciting or accepting anything of value from any person or entity seeking to initiate or maintain a business relationship with the City of Philadelphia, its departments, boards, commissions, and agencies. Contractor understands and agrees that if it offers anything of value to a City official or employee under circumstances where the receipt of such item would violate the provisions of this Executive Order shall be subject to sanctions with respect to future City Contracts. Such sanctions may range from disqualification from participation in a particular Contract to debarment, depending on the nature of the violation. All contractors, agents or intermediaries who are solicited for gifts or gratuities by City employees are urged to report these incidents to the Inspector General, Aramark Tower, Third Floor, 1101 Market Street, Philadelphia, PA 19107.

b. City Employee Interest in City Contracts. In accordance with Section 10-1112 of The Philadelphia Home Rule Charter, no bid shall be accepted from, or Contract awarded to, any City employee or official, or any firm in which a City employee or official has a direct or indirect financial interest. All contractors are required to disclose any current City employees or officials who are employees or officials of the contractor's firm, or who otherwise would have a financial interest in the Contract.

c. Conflict of Interest. Both the State Ethics Act and the City Ethics Code prohibit a public employee from using his/her public office or any confidential information gained thereby to obtain financial gain for himself/herself a member of his/her immediate family, or a business with which he/she or a member of his/her immediate family is associated. "Use of public office" is avoided by the employee or official publicly disclosing the conflict and disqualifying himself/herself from official action in the matter, as provided in The Philadelphia Code Section 20-608.

9. NORTHERN IRELAND, IRAN or SUDAN.

Section 17-104(4)(a) and (b) of The Philadelphia Code prohibits the City from accepting bids from companies that do business in Northern Ireland, Iran and Sudan unless, in the instance of Northern Ireland, that business has implemented the fair employment principles embodied in the MacBride Principles or in the instance of Iran or Sudan, there exists a federal override or the business is excluded from disqualification as described in the Sudan Accountability and Divestment Act of 2007. In furtherance of this ordinance, contractor makes the following certification and representations:

a. In accordance with Section 17-104 of the Philadelphia Code, contractor by execution of its bid certifies and represents that

   i. contractor (including any parent company, subsidiary, exclusive distributor, or company affiliated with Contractor) does not have, and will not have at any time during the term of any Contract (including any extensions thereof), any investments, licenses, franchises, management agreements or operations in Northern Ireland, Iran and Sudan and

   ii. no product to be provided to the City under any resulting Contract will originate in Northern Ireland, Iran or Sudan unless, in the instance of Northern Ireland, Contractor has implemented the fair employment principles embodied in the MacBride Principles or in the instance of Iran or Sudan, there exists a federal override or the Contractor is excluded from disqualification as described in the Sudan Accountability and Divestment Act of 2007.

   In addition to any other remedies reserved under this Contract, any false certification by Contractor is subject to the penalties stated in Section 17-104(c)(3) which include relinquishment of any Bid Security, termination of the Contract and ineligibility for future bids.

10. DISCLOSURES: SLAVERY ERA RECORDS, and FEMALE EXECUTIVES

In accordance with Philadelphia Code Section 17-104 (2), the successful contractor, after award of the Contract, will complete an affidavit certifying and representing that the contractor (including any parent company, subsidiary, exclusive distributor or company affiliated with contractor) has searched any and all records of the contractor or any predecessor business entity regarding records of investments or profits from slavery or slaveholder insurance policies during the slavery era. The names of any slaves or slaveholders described in those records must be disclosed in the affidavit.

The contractor expressly understands and agrees that any false certification or representation in connection with this disclosure and/or any failure to comply with these requirements shall constitute a substantial breach of this Contract entitling the City to all rights and remedies provided in this Contract or otherwise available in law (including, but not limited to, Section 17-104 of The Philadelphia Code) or equity and the Contract will be deemed voidable. In addition, it is understood that false certification or representation is subject to prosecution under Title 18 Pa.C.S.A. Section 4904.

11. MINIMUM WAGE & BENEFITS AND PREVAILING WAGE.

a. If this bid is for the furnishing of services, except where services are incidental to the delivery of supplies or equipment, it is subject to Chapter 17-1300 of The Philadelphia Code and Mayoral Executive Order 03-14 which establish minimum benefits (health benefits and sick leave) and wages for employees. If Contractor and Contractor's first-tier subcontractor(s) furnishing services to the City meet the definition of "Employer," as set forth in Philadelphia Code Sections 17-1302(5) and 17-1303, each shall comply with the minimum wage and benefits provisions established by these laws: from May 20, 2014 through December 31, 2014, the minimum wage shall be $10.88 per hour; on January 1, 2015, the minimum wage shall be $12.00 per hour, which wage amount shall be adjusted annually thereafter, by the CPI Multiplier.* Contractor and its first tier subcontractor(s) shall notify each affected employee what wages are required to be paid. Accordingly, the Contractor, acknowledges and certifies its compliance with Chapter 17-1300 and Executive Order 03-14 and shall also require its first-tier subcontractors to likewise certify and acknowledge their compliance. Contractor shall promptly provide to the City, at its request, all documents and information verifying its compliance and its first-tier subcontractor(s)' compliance with these laws. Any request for a partial or total waiver of these requirements must be based on specific stipulated reasons elaborated in Philadelphia Code Section 17-1304 and should be directed to the attention of the Office of Labor Standards within the City's Managing Director's Office (MDO). Failure to comply with these provisions absent an approved waiver or partial waiver, is an event of default under the Contract and shall also subject Contractor and its first-tier subcontractor(s) to the enforcement provisions in Philadelphia Code Section 17- 1312.

b. The following services require the payment of prevailing wages and submission of certified payroll records under Philadelphia Code Section 17-107 for compensation that exceeds $200,000: landscaping; building care and maintenance; custodial/janitorial housekeeping; security guard service; demolition; snow removal; stucco; roof capping; furniture moving; locking systems and repairs; mechanical/HVAC maintenance and repairs; elevators, escalators, and electrical maintenance and repair, and subcontracts of all or a portion of such contracts. In addition, building service contracts for compensation exceeding $100,000. are also subject to Section 17-107.

*The CPI Multiplier shall be calculated by the Director of Finance for bids issued on or after January 1 of each year by dividing the most recently published Consumer Price Index for all Urban Consumers (CPI–U) All Items Index, Philadelphia, Pennsylvania, as of January of such year, by the most recently published CPI–U as of January 1, 2015.

12. PROTECTION OF DISPLACED CONTRACT WORKERS.

If this contract is for the furnishing of the following services, Security, Janitorial, Building Maintenance, Food and Beverage, Hotel or Non-Professional Health Care Services, then this contract is subject to the "Protection of Displaced Contract Workers" Law, Chapter 9-2300 of the Philadelphia Code. The successful Contractor, if it is a Successor Contractor is required, among other things, to retain certain service employees of the Predecessor Contractor for a ninety-day period.

13. EQUAL BENEFITS.

If this is a Service Contract, as defined in Philadelphia Code Section 17-1901(4), for an amount in excess of $250,000, Contractor shall, for employees providing services under the Service Contract who reside in the City or employees who are non-residents subject to City wage tax under Philadelphia Code Section 19-502(b), extend the same employment benefits the Contractor extends to spouses of its employees to life partners of such employees. By submission of its Bid, Contractor so acknowledges and certifies its compliance with Chapter 17-1900 of the Philadelphia Code and shall notify its employees of the employment benefits available to life partners pursuant to Chapter 17-1900. Following the award of a contract subject to Chapter 17-1900 and prior to execution of the contract by the City, Contractor shall certify that its employees have received the required notification of the employment benefits available to life partners and that such employment benefits will actually be available, or that the Contractor does not provide employment benefits to the spouses of married employees.

Contractor's failure to comply with the provisions of Chapter 17-1900 or any discrimination or retaliation by the Contractor against any employee on account of having claimed a violation of Chapter 17-1900 shall be a material breach the Service Contract.

14. Protected Health Information.

a. The City of Philadelphia is a "Covered Entity" as defined in the regulations issued pursuant to the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The City's business activities include both (1) functions which make the City a Covered Entity, and, therefore, subject to HIPAA, and (2) functions that are not subject to HIPAA.

In accordance with 45 CFR §164.105(a)(2)(iii)(D), the City has designated certain departments and units of the City as health care components that must comply with HIPAA ("Covered Components"). The Covered Components of the City as of August 1, 2013 include: Ambulatory Health Services, a unit of the Philadelphia Department of Public Health ("PDPH"); the Office of Behavioral Health and Intellectual Disability Services; the Philadelphia Nursing Home (a unit of PDPH); the Benefits Administration Unit of the Office of Human Resources; Emergency Medical Services (a unit of the Philadelphia Fire Department); and the Philadelphia Public Health Laboratory (a unit of PDPH). This list is subject to change, and any department or unit of the City that the City in the future determines to be a Covered Component under HIPAA shall be deemed to be a Covered Component for purposes of this Paragraph 32.

b. To the extent (1) this Contract is awarded by the City for or on behalf of a Covered Component and/or requires the performance of services that will be delivered to or used by a Covered Component (whether or not the City department or unit through which the City entered the contract is a Covered Component), and (2) Contractor is a "Business Associate" of the City, as defined in 45 CFR §160.103, the City and Contractor shall negotiate terms and conditions relating to Protected Health Information ("PHI"). The City's published terms are posted at City PHI Terms Relating to Protected Health Information.

15. FORUM SELECTION, CONSENT TO JURISDICTION, AND NOTICES.

The Contract and all disputes arising under this Contract shall be governed, construed and decided in accordance with the laws of the Commonwealth of Pennsylvania. The parties agree that any lawsuit, action, claim or legal proceeding involving, directly or indirectly, any matter arising out of or related to the Contract or the relationship created or evidenced thereby, shall be brought exclusively in the United States District Court for the Eastern District of Pennsylvania or the Court of Common Pleas of Philadelphia County. It is the express intent of the parties that jurisdiction over any lawsuit, action, claim, or legal proceeding shall lie exclusively in either of these two forums. The parties further agree not to raise any objection to any lawsuit, action, claim or legal proceeding which is brought in either of these two forums and the parties expressly consent to the jurisdiction and venue of these two forums. The seller hereby waives trial by jury in any legal proceeding in which the City is a party and which involves, directly or indirectly, any matter (whether sounding in tort, Contract or otherwise) in any way arising out of or related to the Contract or the relationship created or evidenced hereby. This provision is a material consideration upon which the City relied in entering into the Contract. The parties further agree that service of original process in any such lawsuit, action, claim or legal proceeding may be duly affected by mailing a copy thereof, by certified mail, postage prepaid to the addresses specified in the vendor registration in PHLContracts. Any and all other notices by the City may be issued to seller through PHLContracts or by other means to the address provided in seller's Vendor Registration.

16. INSURANCE.

a. Coverage: Unless otherwise approved by the City's Risk Management Division in writing, Contractor shall, at its sole cost and expense, procure and maintain, or cause to be procured and maintained, in full force and effect throughout the term of this Agreement or otherwise as specified below, the types and minimum limits of insurance specified below, covering Contractor's performance of the Services and the delivery of the Materials. Contractor shall procure, or cause to be procured, all insurance from reputable insurers (meaning those with an AM Best rating of A-, Class VII or above) admitted to do business on a direct basis in the Commonwealth of Pennsylvania or otherwise acceptable to the City. All insurance herein, shall be written on the basis shown below. In no event shall Contractor perform any Services or other work until Contractor has delivered or caused to be delivered to the City's Risk Management Division the required evidence of insurance coverages. In the event coverage is cancelled, or non-renewed, Contractor shall promptly provide written notice to City. The City, its officers, employees, and agents shall be named as additional insureds on the General Liability Insurance policy. Contractor shall also evidence on an Acord Certificate of Liability Insurance Form that the coverage afforded the City and its officers, employees and agents, as additional insureds on the General Liability policy, will be primary to any other coverage available to them and subject to the terms of such coverage.

(1) Workers' Compensation and Employers' Liability:

(i) Workers' Compensation: Statutory Limits.

(ii) Employers' Liability: $100,000 Each Accident - Bodily Injury by Accident; $100,000 Each Employee - Bodily Injury by Disease; and $500,000 Policy Limit - Bodily Injury by Disease.

(iii) Other state's insurance required by the Laws of the Commonwealth of Pennsylvania applicable to Contractor as a provider of information technology products and services.

(2) General Liability Insurance (per occurrence and in the aggregate):

(i) Limit of Liability: $1,000,000 per occurrence combined single limit for third party bodily injury (including death) and property damage liability; $1,000,000 advertising injury; $2,000,000 general aggregate and $1,000,000 aggregate for products and completed operations. The parties may discuss higher limits of liability if, their mutual determination, the potential risk warrants.

(ii) Coverage: Premises operations; blanket contractual liability; personal injury liability; products and completed operations; independent contractors; employees and volunteers as insureds; cross liability; and broad form property damage (including completed operations).

(3) Automobile Liability Insurance:

(i) Limit of Liability: $1,000,000 per occurrence combined single limit for bodily injury (including death) and property damage liability.

(ii) Coverage: Owned, non-owned, and hired vehicles

(4) Professional Errors & Omissions Insurance:

(i) Limit of Liability: $2,000,000.

(ii) Coverage: Errors and omissions including liability assumed under Contract.

(iii) Professional Liability Insurance may be written on a claims-made basis. If written on a claims-made basis. Contractor agrees to maintain insurance or tail coverage, for a period of at least two (2) years after expiration or termination of this Contract as long as such coverage remains commercially available for purchase.

(a) Inclusion of network security and privacy liability in Professional E&O Insurance:

(i) Limit of Liability: $2,000,000 Per Claim/Aggregate

(ii) Coverage: Information security and privacy liability that arise from the Agreement, if these costs are incurred by the City due to mistakes or errors made by IBM, including but not limited to: data while in transit or in the possession of any third parties hired by the Contractor (such as data back-up services) to electronic system; loss of, damage to or destruction of electronic data breaches arising from the unauthorized access or exceeded access; or malicious code, viruses, worms or malware; electronic business income and extra expense as a result of the inability to access website due to a cyber attack or unauthorized access; privacy notification extra expense coverage (including Credit Monitoring Expense).

(iii) reserved.

(iv) reserved.

(b) Evidence of Insurance Coverage. Certificates of insurance evidencing the required coverages must specifically reference the City contract number for which they are being submitted. The original certificates of insurance must be submitted to the City's Risk Manager at the following address:

The City of Philadelphia
Office of the Director of Finance
Division of Risk Management
1515 Arch Street, 14th Floor
Philadelphia, PA 19102-1579
(Fax No.: 215-683-1705)

A copy of the certificates of insurance shall be submitted to the City's Primary Contract at the address of the Department set forth above. Both submissions must be made at least ten (10) days before work is begun and at least ten (10) days before any renewal or extension of the term of the Contract. The City, in its sole discretion, may waive the ten (10) day requirement for advance documentation of coverage in situations where such waiver will benefit the City. The actual endorsement adding the City as an additional insured must specifically reference the City contract number and be submitted to the Participating Entity at the above address. The City reserves the right to require Contractor to furnish written responses from its authorized representatives to all inquiries made pertaining to the insurance required under the Agreement at any time upon fifteen (15) days written notice to Contractor..

(6) IBM subcontractors used in the performance of this contract shall maintain insurance coverages of the types and in the amounts customary for businesses of similar size and in accordance with industry practice.

Attachment A

Indemnification and Limitation of Liability

.

1. INDEMNIFICATION AND LIMITATION OF LIABILITY: NEGOTIATED

Items for Which IBM May Be Liable

The Contractor shall indemnify, keep and save harmless, and defend the City of Philadelphia, its officials, employees and agents ("City Indemnitees") against third party suits or claims by paying all related damages awarded, settlement payments agreed to by Contractor, attorneys' fees, costs, expenses, or liabilities where such claim alleges personal injury (including bodily injury and death) for which Contractor is legally responsible or damage to tangible personal property for which Contractor is legally responsible, and where caused by Contractor's negligent acts or errors or omissions or the negligent act or error or omission of Contractor's, subcontractors, independent contractors, or employees in connection with this Contract.

Further, Contractor shall indemnify City Indemnities from Data Breach Damages (as defined below) (provided Contractor's financial responsibility for Data Breach Damages in all cases shall be limited to the Data Breach Damages Cap set forth below and recovery under this paragraph shall reduce the Data Breach Damages Cap on a dollar-for-dollar basis). Contractor's indemnification obligations under this Agreement shall be excused in the event Contractor is not given timely written notice by the City of any suit or claim, and City shall allow Contractor to control to the extent approved by the City Solicitor, which will not be unreasonably withheld and the City shall reasonably cooperate with Contractor in the defense and any related settlement negotiations. If the City Solicitor does not give such approval, IBM has no obligation to defend the City as set forth above.

Circumstances may arise where, because of a default on IBM's part or other liability, City is entitled to recover damages from IBM. Regardless of the basis on which City is entitled to claim damages from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM's entire liability for all claims in the aggregate for actual, direct damages will not exceed the amount of $10,000,000. Notwithstanding the foregoing, this limitation shall not apply to liability for damages resulting from loss of life, bodily injury or damage to real and/or tangible personal property, or Data Breach Damages as defined in the paragraph below which instead shall be subject to the cap set forth therein, and/or infringement of proprietary right as set forth in the Intellectual Property Section below.

Upon notice by the City, Contractor shall reimburse the City within 30 days for (i) legally required notification costs, (ii) credit monitoring costs for up to twelve (12) months or such longer time as legally required, (iii) reasonable costs of incident investigation, and (iv) judgments awarded to affected data subjects as part of third party claims brought against the City ("Claims"), or settlements approved by Contractor to resolve such Claims (collectively "Data Breach Damages") arising out of an unauthorized disclosure of personal information caused by Contractor's breach of its security obligations related to such data hereunder as set forth in Exhibit A, IBM Data Security and Privacy Principles for Technology Support Services. Contractor's total liability for such Data

Breach Damages shall not exceed $5,000,000, ("Data Breach Damages Cap") and in all cases shall be limited to Contractor's proportional fault in causing such unauthorized disclosure. Additionally, Contractor shall have no responsibility for damages that could have been prevented by implementing reasonable security measures recommended by Contractor that City opted not to implement as part of the Services.

For purposes of this Limitation of Liability section, the term "Product" also includes Materials and Machine Code. This limit also applies to any of IBM's subcontractors and Program developers. It is the maximum for which IBM and its subcontractors and Program developers are collectively responsible. The following amounts are not subject to a cap on the amount of damages:

a. payments referred to in the Intellectual Property Protection section below; and
b. damages for bodily injury (including death) and damage to real property and tangible personal property for which IBM is legally liable.

Items for Which IBM Is Not Liable
Except as expressly required by law without the possibility of contractual waiver, under no circumstances is IBM, its subcontractors, or Program developers liable for any of the following even if informed of their possibility:

a. reserved; special, incidental, exemplary, or indirect damages or for any economic consequential damages; or
b. lost profits, business, revenue, goodwill, or anticipated savings.

This clause shall not be construed to bar any legal remedies the Contract Vendor may have with the State's failure to fulfill its obligations pursuant to the Master Agreement.
For purposes of this Intellectual Property Protection section, the term "Product" also includes Materials and Machine
Code.

Intellectual Property Section
If a third party asserts a claim against Customer that an IBM Product that IBM provides to Customer under this Agreement causes property damage, personal injury, death or infringes that party's patent or copyright, IBM will defend Customer against that claim at IBM's expense and pay all costs, damages, and attorney's fees that a court finally awards against Customer or that are included in a settlement approved in advance by IBM, provided that Customer:

a. promptly notifies IBM in writing of the claim;
b. allows IBM to control, and cooperates with IBM in, the defense and any related settlement; and is and remains in compliance with the Product's applicable license terms and Customer's obligations under the remedies section) below.

Remedies

If such a claim is made or appears likely to be made, Customer agrees to permit IBM, in IBM's discretion, either to i)enable Customer to continue to use the Product, ii) modify it, or iii) replace it with one that is at least functionally equivalent. If IBM determines that none of these alternatives is reasonably available, then on IBM's written request, Customer agrees to promptly return the Product to IBM and discontinue its use. IBM will then give Customer a credit equal to:

a. for a Machine, Customer's net book value calculated according to generally-accepted accounting principles;
b for an ICA Program, the amount Customer paid IBM for the Program's license or 12 months' charges (whichever is less); and
c. for Materials, the amount Customer paid IBM for the creation of the Materials.

Claims for Which IBM is Not Responsible
IBM has no obligation regarding any claim based on any of the following:

a. anything provided by Customer or a third party on Customer's behalf that is incorporated into a Product or IBM's compliance with any designs, specifications, or instructions provided by Customer or a third party on Customer's behalf;
b. a Product's use other than in accordance with its applicable licenses and restrictions or use of a non-current version or release of a Product, to the extent a claim could have been avoided by using the current release or version;
c. any modification of a Product made by Customer or by a third party on Customer's behalf or the combination, operation, or use of a Product with any other Product, hardware device, program, data, apparatus, method, or process;
d. distribution/use of product outside customer's enterprise;
e. non IBM product or other IBM program.

This intellectual property section states IBM's entire obligation and Customer's exclusive remedy regarding any 3'" party Intellectual property claims.

IBM Data Security and Privacy Principles for Technology Support Services

Contents

1. Data Security and Privacy Review

This Data Security and Privacy Principles for Technology Support Services, is restricted in scope to the description of the handling and protection of Client Data by IBM in its provision of Technology Support Services (TS Services or TSS). It describes the general set of principles, processes, controls, and tools that IBM uses in its internal data processing facilities with respect to Client-owned data provided by the Client identified in the transaction documents or otherwise collected by IBM in the provision of post sales technical support provided by IBM (collectively, “Client Data”).

Legal Compliance

IBM will comply with all laws and regulations applicable to its TS Services, including those applicable to security breach notification. IBM does not make the determination whether data sent to IBM by the Client to assist in problem determination includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Handling Process documented below.

Updates to Data Security and Privacy Principles (DSPP) for TS Services

When IBM supplements, modifies, or changes the scope of those TS Services through the documented change management process, IBM may provide new terms or make updates to the DSPP in accordance with those changes. When a Client renews or purchases a new TS Service, the then-current DSPP will apply to the Client’s subscription for those TS Services.

Client Data

Client Data defined. Client Data is an asset that originates with the Client and is provided to IBM to access, store or manage as part of an accepted TS Services contract. Client Data can come into IBM’s possession in several ways, for example: (1) Clients ma**y** use IBM product support offerings, (2) Clients may send structured or unstructured data for use in post-sales Technical Support Services problem determination (e.g., debugging data such as contained in storage dumps), and (3) Clients may return machines or machine parts for upgrade, exchange, or repair, and th**at** equipment may contain Client Data.

Use of Client Data. Client Data will be used only to provide the Client with TS Services - including activities compatible with providing those TS. IBM will not use Client Data or derive information from Client Data for any other commercial purposes without Client’s permission.

Disclosure of Client Data. To TS Support, IBM at times uses its subsidiaries and business partners as sub-processors in post sales TS Services and will share Client Data with those sub-processors as required. Otherwise, IBM will not disclose Client Data outside of IBM, its subsidiaries or business partners except as the Client directs, or as required by law.

Processing of Client Data. The European Union General Data Protection Regulation (“GDPR”) requires agreements between a controller and processor, and between a processor and sub-processor, so that processing is performed in accordance with the processor’s Technical and Organizational Measures (“TOMs”), and to ensure the protection of the rights of data subjects in accordance with the GDPR. IBM makes the commitment to the GDPR Provisions to all Clients effective May 25, 2018.

Provisions for the European Union General Data Protection Regulation

1) The processor provisions of the GDPR apply to the processing of Client Data within the scope of the GDPR by IBM, on behalf of the Client.

2) For purposes of the processor provisions of the GDPR, the Client and IBM agree that the Client is the controller of Client Data and that IBM is the processor of such data; when the Client acts as a processor of Client Data, IBM is a sub-processor.
3) The processor provisions of the GDPR do not apply where IBM is a controller of Client Data.
4) The processor provisions of the GDPR do not limit or reduce any commitments that IBM makes for data protection to the Client in any other agreement between IBM and the Client.

2. Data Processing Security Principles

IBM highly prioritizes Client Data security. The security of facilities, people, and data are all ingrained into the business controls that guide the organization. This section describes some of the underlying security principles that inform IBM security policies and procedures.

IBM has long focused on security through the use of hardware and software configurations**,** and through the design and implementation of business processes and practices. Threats can originate inside or outside an organization, so IBM's security procedures and practices consider a broad range of potential risks to data security, including technological, human, and natural sources.

The internal IBM Corporate Instruction for Information Technology (IT) security was developed decades ago and has undergone many revisions. It provides an oversight and control structure for: risk analysis, physical security, access management, emergency planning, investigations, Information protection, education, and more. It documents guidelines and requirements for IT security and the protection of data, including Client Data. Some of the requirements documented in that Corporate Instruction (and elsewhere) are summarized in this DSPP.

Compartmentalization

Compartmentalization is a technique that helps control risk associated with human behavior, and is the act of limiting data access, both physical and logical, to those personnel who genuinely need such access to perform their jobs. IBM limits physical and logical access to data centers, for example, to those personnel with a business need for access to perform their jobs. IBM limits logical access to applications and databases, to authorized personnel whose job function requires access.

Least Privilege

The Principle of Least Privilege states that personnel who access should have the least amount of access necessary to perform their job function. This Principle is applied to both physical and logical access to data, and the systems and applications that process data. The ability to Read, Create, Update and Delete data are all access controls subject to the principle of Least Privilege.

Separation of Duties

Separation of Duties ("SoD") is a basic internal control which avoids a conflict of duties by directing that no one individual has responsibilities or access that would allow the individual to misuse or divert company assets without deterrence or timely detection. TS Services implements SoD concepts in accordance with IBM's Corporate Instruction though a combination of process design, system controls, and organizational structure. (Reference the "Media and Physical Disposal of Media" topic in Section Three for one application of this control.)

Defense in Depth

Defense in Depth refers to the practice of creating multiple layers of security, for example physical Defense in Depth is requiring badge access to a building, followed by badge access to a data center, then separate access control to server cages within the data center.

Logical Defense in Depth is for example, multiple layers of firewall protection as described in more detail later in this document.

Privacy by Design

Privacy by Design means that data protection principles are incorporated into the design of a processing activity from the start of Services and are considered throughout the lifecycle of each offering.

As noted in the definition of Client Data, IBM may receive unstructured or unformatted data (i.e. data storage dumps or screen shots) from a Client to assist IBM personnel in providing TSS post-sales support. The content of this unstructured data may be unknown to either the Client or IBM at the time of transmission, and so may contain any data element defined in our standard taxonomy of personal data. IBM will implement TOMs to limit its processing of Client Data to the permitted purposes. Only authorized IBM personnel and authorized sub-processors who need access to undertake authorized tasks compatible with permitted purposes will be given access to Client Data.

IT Risk Management

Risk assessment and risk management are fundamental foundations of data security. IBM's internal business controls staff periodically audits applications and processes for business controls compliance.

IBM also has an IT Risk Management Steering Committee headed by the IBM Chief Information Officer ("CIO"). Members of the committee are security professionals, executives, and people who create internal IT standards for management approval. This committee continually examines IT risks across a broad spectrum of potential threats. The output of this committee is used to improve IBM's IT risk posture.

3. Physical Security

Facilities and Access Control

Physical security is a key aspect of protecting Client Data. IBM employs access control mechanisms to limit access to system assets and infrastructure components. Keys, cipher locks, electronic controlled access systems, guarded entrances, and in some cases biometric controls are all examples of physical access control that may be employed by IBM. For instances where a Controlled Access area ("CA") is located in a non-IBM owned facility, security requirements are detailed by contract and the owner of that facility agrees to comply with those requirements.

CAs are categorized according to a set of CIO defined criteria to identify and protect facilities, contents, and people. Access to CAs are logged and the logs are reviewed either by automated tools or manually according to IT security guidelines. Documentation including security review evidence is required to be kept according to IBM worldwide records management policies.

Every CA has an identified owner responsible for following security policies. CAs are required to be locked even when occupied. Site specific security procedures applicable to a CA are required to be documented and tested. Personnel are given authorized physical access to CAs only with business justification. Depending on that person's job responsibilities, access may be restricted to only a portion of the facility.

Media and Physical Disposal of Media

Server media used for backup, records retention, or disaster recovery is required to be physically protected against unauthorized use, theft, and damage. Only approved carriers are used to transfer electronic media that may contain unencrypted data.

Server storage Media Custodians that handle Client Data are responsible for accurate media inventory and for reporting any discrepancies according to and using IBM's **Security Incident Handling Process** (SIHP). In keeping with the separation of duties security principle, at least one person not involved in the media operation must perform the inventory (the Storage Media Custodian may participate, but is not permitted to be solely responsible for performing the inventory).

Machine**s** or machine parts returned to an IBM for upgrade, exchange, or repair that contain Client Data must be securely erased by the Client to render the data unrecoverable before shipment. If the Client is unable to perform this task for any reason, IBM offers secure erasure or media retention services for a fee.

4. Logical Security

Logical security consists primarily of technical measures. A few common logical security measures apply to networking infrastructure, servers, and workstations. These measures include access controls (more details in individual sections below) and technical measures to address propagation or execution of unapproved code (e.g., viruses and other malware). Updates are done automatically wherever possible (such as workstation antivirus updates) or periodically on a prescribed, prioritized schedule. Examples of logical security include:

- Periodic vulnerability scans and penetration testing.
- Patch management is required to be done on a timely basis, based on a classification scheme of systems and the severity level of the patch, and sometimes even based on the operating system type or release.
- Technical controls to prevent denial of service attacks (primarily applicable to network infrastructure and servers).
- Creation and capture, if the device is capable, of activity logging records (network infrastructure and servers) that can be accessed for audit and by "suspicious activity" monitoring tools. The length of time such log records must be kept is determined by IBM Worldwide Records Management (WRM), which categorizes and details retention requirements. A list of suspicious activities to be monitored is maintained by CIO.
- Requirement to follow specific security measures for remote access to IBM internal systems from outside the logical firewall, including a mandatory VPN client. All such access is encrypted. (Applicable to workstation and mobile devices);
- Requirement that devices are to be cataloged in a database used for control and audit purposes.
- Requirement to use static IP addresses (DHCP/DDNS are generally not permitted, except in some approved and documented cases for servers, and for workstations generally). All static IP addresses are recorded in a secure database;
- IBM requires an acceptable use policy be readily available to users and represented each time conditions change, asking confirmation that the user has read and understood the terms for the data that may be stored or processed there;
- Requirement to use specific CIO guidelines to build operating system images (workstations or servers); and
- Requirement to undergo security health checks as part of a broader independent audit process.

Where permitted by law, Security Technical Testing (STT) is performed by teams of individuals with highly specialized skills who are allowed to use their skills, tools, and techniques to discover potential exposures that would not normally be found during routine testing. This is sometimes referred to as white hat testing or ethical hacking. There are established resources within IBM to assist individuals performing STT, including process overview documentation.

Technical Specifications for Servers, Middleware, and Applications

IBM maintains detailed technical specifications for security that are specific to each operating system, each middleware product, and deployed applications. All production servers, middleware and application code used to provide post sales technical support will meet or exceed the specifications defined by the CIO.

Role Based Access

IBM's internal security services have in place an access control policy that describes the security requirements based on the type of data contained in the system, a user's need to know, legal and/or contractual obligations. Approval, review and removal of access requests are formally defined with those considerations in mind. IBM maintains an audit trail of all significant events concerning access rights and managing identities.

Password and authentication Policy

IBM production systems require authentication for access. This includes network devices, servers, workstations, and some types of applications. Some systems require user ID and password or digital certificate while others require multi-factor authentication ("something you know plus something you are or have," such as password plus biometric scan, or password plus security key fob). Multi-factor authentication is required for any system available over a public network or for any privileged user with system authority.

Password rules apply. Passwords are required to be of a certain length and contain certain combinations of letters, cases, numbers, and other special characters. In addition, incorrect password attempt rules are in force, such as disallowing access after a certain number of incorrect attempts. Automated tools (where possible) remind users to change passwords and enforce the password rules.

Non-expiring passwords are generally not allowed, with very limited exceptions (e.g., laptop hard drive passwords are exceptions, but these passwords only come into play if a drive is removed and reconnected to a "foreign" controller). Digital certificates used for identification must be from an IBM CIO-approved certificate authority.

Network Security

Network security involves both physical and logical security measures. From a logical security perspective, IBM partitions its IT infrastructure into security zones with flow control devices, such as firewalls and routers, governing the allowable flows between security zones. This enables IBM to deploy an architecture conforming to the Defense in Depth security principle described above.

Physical security restrictions exist as to physical placement of network infrastructure devices inside CAs. Any system connecting to an untrusted network, such as the Internet, is highly restricted. Connections from these highly restricted systems to any other production systems in IBM are tightly controlled. Firewalls are specified at several levels in the network architecture. Required firewall rule sets are maintained.

Technical controls to restrict the propagation or execution of unapproved code (e.g., viruses or other malware) are required for any infrastructure device, where possible. Routers, switches, wired and wireless access points are access controlled, as are servers and workstations. No unsecured wireless access points are permitted (with limited exceptions for unsecured guest access to the Internet). Access by authorized personnel is limited to those whose job role requires access. General users are not allowed access to network infrastructure devices.

Server Security

Logical and physical controls apply to production server systems. Many technical controls are required for server systems, based on server use categorizations. The IBM CIO maintains a set of hypervisor security rules and extensive detailed technical specifications for security settings by server OS.

Server access is based on need. As elsewhere, server authorization rules follow the principle of least authority, where the lowest level of authority consistent with the business need is granted. In particular, general users are not granted "super user" or equivalent privileges on production servers.

Server administrators or anyone having administrative access privileges are subject to more security requirements than general users.

Database Security

The IBM CIO maintains extensive detailed technical specifications for security settings for database middleware. Databases, like servers in general, have physical and logical control requirements. Databases are required to have several levels of access controls, which can also vary by the sensitivity of the data kept within them. Database administrators, as with other elevated privilege users, are subject to more security requirements than general users.

Workstation and Portable Device Security

IBM employees are required to follow specific rules concerning workstations potentially used to access Client Data. Workstations:

- Must have up to date anti-virus protection proscribed by CIO (specific anti-virus software is mandated). Virus scans are required and automatically scheduled;
- Must have log on password protection enabled;
- Must have keyboard / screen lock timeout set to 30 minutes or less (in some cases 15 minutes);
- Must use the encryption option for any Lotus Notes databases that could contain sensitive information;
- If the device supports a hard drive password it must be enabled, unless full disk encryption is used;
- Must be automatically kept current with security patches;
- Must not contain unapproved or inappropriate software or data;
- Can only use pre-approved open source software. The approval process is intended to insure that only tested and safe software is used and IBM complies with applicable terms of use;
- Must have special monitoring software programs installed that can verify compliance with security requirements and help IBM to manage end use devices (for example, Tivoli End Point Manager);
- Must have specific, CIO approved Virtual Private Network (VPN) software installed to remotely access the IBM intranet. Such access is encrypted to CIO-specified strength;
- Must have an IBM-approved client firewall installed and operating;
- Must not use Internet peer-to-peer file sharing applications, unless approved by CIO;
- Must not allow any form of unauthenticated or unapproved access;
- Must have a registered MAC address; and
- Obtain approved versions of IBM required software from an internal software distribution system (called ISSI, IBM Standard Software Installer).

IBM maintains the right to confiscate any personally owned asset (such as laptops or cell phones) that are used or partly used for IBM business purposes. Such confiscations can be made, for example, to aid an investigation.

Application Security

Application administrators are subject to additional security requirements than general users, due to their enhanced authority level. Production applications require authentication and authorization, similar to but distinct from operating system log on.

Intrusion Prevention, Detection, and Vulnerability Scanning

Intrusion prevention is required. Anti-malware software controls are required at several levels (several levels in the network architecture, server, and workstation). Firewalls are specified at several levels within the network infrastructure as well as for servers and workstations.

Detecting suspicious activity is required. Many activities and accesses are monitored and logged to support suspicious activity detection. Users with elevated privileges are monitored to a higher degree. A list of required security log events is maintained by CIO.

Vulnerability scanning is performed according to a schedule related to the type of system being scanned. Internet facing systems found to have a vulnerable condition are removed from service unless they can be corrected with specified time limits.

Approved scanning tools are available for system administrators and security professionals to download from the internal Security, Asset, and Risk Management ("SARM") web site. Required vulnerability scan profiles are also kept there.

5. Secure Engineering

The IBM Secure Engineering Framework reflects commercially reasonable efforts and directs development teams to give proper attention to security during the development lifecycle.

Secure Engineering practices include: project planning, security awareness education, risk assessment & threat modeling, security requirements, secure coding, source code scanning & dynamic security testing, security documentation and a product security incident response process. These practices are intended to help enhance product security, protect IBM intellectual property, and support the terms of warranty of IBM products. For more about IBM product security, see:

http://www.ibm.com/security/secure-engineering/ http://www.ibm.com/security/secure-engineering/process.html

6. Security Incident Handling Process

IBM maintains a common single security incident reporting and mitigation system in which IT security and data incidents which may involve a compromise of: (1) either personal information, client information, IBM confidential, technical or scientific information; or (2) a productivity device; or (3) suspicious IT activity; or (4) a suspected system penetration is reported to a single phone or web contact point.

This report initiates a response from a 24x7x365 team of specifically trained and equipped employees who, working with the software business teams and other subject matter experts as needed, will manage the incident until resolution.

Subject matter incident responders have been identified for each business area, so if an incident occurs, a Security Incident Handling Process ("SIHP") is also invoked to ensure that a rapid, response to security incidents, aligned with corporate reporting requirements, takes place.

IBM supports the GDPR reporting requirements and will report any data breach within 72 hours acting in either a controller or processor role. Those reporting requirements will include:

- a description of the nature of the Client Data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the Client Data breach; and,
- the measures taken or proposed to be taken by the controller to address the Client Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7. Employment Practices Related to Data Security

Protecting Client Data depends on technical and other means as described earlier, and on the workforce that manages the data. Employment practices are designed to make sure that all employees and contractors meet a set of guidelines and can be, to the extent consistent with applicable law, monitored in their work-related activities.

Hiring and Separation Policies

Where permitted by law, pre-employment screening includes background checks, verification of claimed educational status, verification of government issued photo ID, and verification of other employment application claims. Separation policies require removal of network access (target less than 24 hours). Separating employees are required to return IBM property including workstations, laptops, IBM owned media, and any communication equipment. Separating employees are reminded of their continued obligation to data confidentiality.

Training and Culture

New employees receive training, which includes proper use of IT assets and protection of sensitive data. Annual CIO specified training in digital threats and security is required of all employees.

Compliance with Policies

IBM maintains an employee code of conduct including Business Conduct Guidelines (BCGs). These are administered by the IBM General Counsel. The BCGs require that IBM employees conduct business using high ethical standards and in accordance with data security and confidentiality policies. Employees are encouraged to report illegal or unethical behavior or even the appearance of it.

Employees must read and agree to abide by the BCG upon hiring and every year thereafter. Compliance with the BCGs is a condition of employment. IBM makes the BCGs available publicly at:

http://www.ibm.com/investor/governance/business-conduct-guidelines.wss

Confidentially Speaking

In order to protect Client Data, employees may bring problems to management attention at any time. IBM has established programs to enable this freedom to identify and report any potential issue.

8. Corporate Controls, Corporate Instructions, CIO Standards

IBM uses the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") framework and its five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring.

Policies and uniform practices are established in the form of corporate directives which are IBM’s primary method for documenting and effectively communicating its policies, delegations, and instructions to IBM management and employees. IT Security policies derive their authority from specific CIs and other authoritative business control sources as above and as such are an integral part of IBM’s business.

9. Audit

Client Data security depends on controls being implemented and verified. One way **that** verification is achieved is through audits independent of the unit performing work. IBM routinely audits for compliance with business controls, including IT controls (auditing that security standards and policies are in compliance). The Business Controls and Internal Audit function report to the IBM CFO, who is accountable to the Audit Committee of the Board of Directors.

10. Business Continuity

All functions critical to the operation of IBM’s business have disaster recovery (“DR”) plans. These formal plans are documented and annually (at least) revalidated. Technical support problem reporting and resolution services, which depend on Client Data, are critical and have DR plans.

11. Crisis Management

IBM maintains a Crisis Management process under an Emergency Planning Program, designed to enable IBM to address crises as they arise. The process requires IBM sites/locations with personnel to create an Emergency Plan. The Crisis Management process is activated immediately when an actual or potential crisis situation arises.

12. Service and Support

Clients may be asked to provide (or may choose to voluntarily send) data to IBM to aid in debugging a problem. Clients will be asked to use the secure online tool known as Enhanced Customer Data Repository (ECuRep”) to send debugging data to IBM. The ECuRep tool and its terms of use are described here: http://www.ibm.com/de/support/ecurep

13. Acquisitions

IBM may acquire other companies with existing Client Data security policies and procedures that differ from IBM’s. Acquired companies are required to comply with the same security policies as IBM within a defined integration or transition period after the acquisition. The same physical, logical, and business controls that are applied across IBM will apply to the acquired company by the end of the integration period. The length of time required for the integration period depends on the complexity of the acquired company’s existing infrastructure.

DocuSign
SECURED

Certificate Of Completion

Envelope Id: 890CFC5E607F4BA9A3A74C79E05C10AE

Status: Completed

Subject: Please DocuSign: City of Philadelphia - IBM NASPO Contract MNWNC-final clean with Exhibt A.pdf

Source Envelope:

Document Pages: 25	Signatures: 3	Envelope Originator:
Certificate Pages: 3	Initials: 0	City of Philadelphia - Commercial Law Department
AutoNav: Enabled		1234 Market Street
EnvelopeId Stamping: Enabled		Suite 1800
Time Zone: (UTC-05:00) Eastern Time (US & Canada)		Philadelphia, PA 19107
		commercial.law@phila.gov
		IP Address: 173.49.99.30

Record Tracking

Status: Original 7/23/2020 6:53:44 PM	Holder: City of Philadelphia - Commercial Law Department commercial.law@phila.gov	Location: DocuSign

Signer Events	Signature	Timestamp
KA Schneider kasch@us.ibm.com NASPO Program Manager Security Level: Email, Account Authentication (None)	DocuSigned by: KASchneider 57D3F4927D58417... Signature Adoption: Uploaded Signature Image Using IP Address: 107.210.172.166	Sent: 7/23/2020 7:01:25 PM Viewed: 7/28/2020 5:33:20 PM Signed: 7/28/2020 5:34:02 PM
Electronic Record and Signature Disclosure: Accepted: 7/28/2020 5:33:20 PM ID: 90678500-033a-4b98-90d0-8a052197c760		
Phillip Bullard phillip.bullard@phila.gov Senior Attorney City of Philadelphia Security Level: Email, Account Authentication (None)	DocuSigned by: Phillip Bullard D53E7FF627014D0... Signature Adoption: Pre-selected Style Using IP Address: 173.49.99.30	Sent: 7/28/2020 5:34:03 PM Viewed: 7/29/2020 11:53:49 AM Signed: 7/29/2020 11:54:06 AM
Electronic Record and Signature Disclosure: Accepted: 7/29/2020 11:53:49 AM ID: ed241d10-d7d6-4612-b22d-f4af0ae90e63		
Monique Nesmith-Joyner Monique.Nesmith-Joyner@Phila.gov Procurement Commissioner City of Philadelphia Security Level: Email, Account Authentication (None)	DocuSigned by: Monique Nesmith-Joyner 31897BB77B8C4BB... Signature Adoption: Pre-selected Style Using IP Address: 100.14.15.36	Sent: 7/29/2020 11:54:07 AM Viewed: 7/29/2020 6:45:02 PM Signed: 7/29/2020 6:45:09 PM
Electronic Record and Signature Disclosure: Accepted: 3/4/2019 11:45:50 AM ID: 9e2fd9e4-dd4e-4a8b-9ae0-14dfbad9cab2		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/29/2020 11:54:07 AM
Certified Delivered	Security Checked	7/29/2020 6:45:02 PM
Signing Complete	Security Checked	7/29/2020 6:45:09 PM
Completed	Security Checked	7/29/2020 6:45:09 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

Electronic Record and Signature Disclosure created on: 9/5/2016 1:40:22 AM
Parties agreed to: KA Schneider, Phillip Bullard, Monique Nesmith-Joyner

This Electronic Records and Signature Disclosure is provided by the City of Philadelphia in connection with a pending electronic transaction. Any party proceeding with such electronic transaction is deemed to have consented i) to conduct the transaction by electronic means; and ii) where execution of an agreement is required, to the use of electronic signatures using the method provided in the agreement. Questions regarding this Electronic Records and Signature Disclosure should be addressed to econtractphilly@phila.gov.