ADDITIONAL IT STANDARDS

DATA REQUIREMENTS, ADDRESSING, DIGITAL AND WEB CONTENT ACCESSIBILITY

If applicable, applications or solutions proposed by vendors must be in alignment with these City's Standards:

Section 1

Data Requirements Standards - All City solicitations that include the purchase of software or services relating to information systems must incorporate the requirements of this policy. This document defines standards to guide implementation of the following current and future policies covering third-party access to City information:

- Data Access Requirements for Third Party Systems
- Master Data Requirements
- Metadata Standards
- Date Formats
- Common Data Elements for Geospatial Data
- Data Protection and Retention

Section 2

Addressing Standards should be adopted for use within all database systems, applications or tables that maintain a property address.

Section 3

General Technical Standards - The City's standard non-functional requirements for IT systems ensure that information systems are resilient and secure so that the City's information is safeguarded, and its staff can continue operations (as supported by IT systems) in the event of a disaster.

Section 4

Digital Standards provide the design, code, and content guidelines for City website and web application development;

Section 5

Web Content Accessibility Standards - All sites produced by vendors for the City, regardless of the hosting environment, shall conform to the Web Content Accessibility Guidelines (WCAG) 2.1 AA. These guidelines will make content more accessible to a wider range of people with disabilities.

Section 6

Security Addendum - 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.

Office of Innovation & Technology

Section 1

Third Party Data Access Standards

SOP No:	SOP Type:	Family:	Internal [ ]	Version:
1010	Standard	System and Services Acquisition (SA)	External [x]	1.0
Category:	Originating Unit(s):		Effective Date:	Review Cycle:
System Acquisition	Enterprise Architecture		8/24/2020	Annual
Supersedes:	Forms:	Attachments:	Contact:	
N/A	[ ] Yes [x] No	[ ] Yes [x] No	Chief Enterprise Architect	

Contents

1 Purpose 1
2 Scope 2
3 Policy 2
4 Standards 2
5 Roles and Responsibilities 6
6 Compliance 6
7 Guidance 7
8 Waivers 7
9 Definitions 7
10 Authority 7
11 Related Links 7
12 Change Log 8
13 Approval 8

1 Purpose

- Ensure City ownership of data in proprietary systems.

- Assist decision makers, project teams, procurement, and legal departments by clearly defining the expectation of data ownership in vendor systems and related data access capabilities to be considered before choosing a solution.

2 Scope

All City solicitations that include the purchase of software or services relating to information systems must incorporate the requirements of this policy.

3 Policy

This document defines standards to guide implementation of the following current and future policies covering third-party access to City information:

- System and Services Acquisition.

4 Standards

4.1 Data Access Requirements for Third-Party Systems

The City considers all information that is generated or stored in third-party information system to be City property.

In accordance, the City requires perpetual, non-proprietary means to access data in third-party systems implemented by the Applicant or associated Parties.

Examples of non-proprietary means include:

1. A documented and secured web-based Application Programming Interface that meets City standards. The Current City standard API specification is RESTful web services with JSON payload.
2. Secure access to databases using non-proprietary client software that follows ODBC specifications. Documentation of database elements that store City data. Open Database Connectivity is the City's standard API for directly accessing database management systems.
3. Secure access to file systems where City information is stored.
4. Other means of securely providing third-party system data to the City, including exporting flat files.

Proposals shall include a statement of the Applicant's ability to provide access to data in the context of the choices above. The City may consider alternative means on a case-by-case basis.

If these means of access are available through proprietary components of the third-party system, the vendor shall provide, free of charge, an agreed upon amount of service

accounts to be used solely for programmatic retrieval of data. The vendor will contractually agree to provide access to data when a given vendor system is replaced or usage is terminated.

Electronic documents stored in proposed third-party systems shall be exportable in non-vendor proprietary formats, including but not limited to:

- Adobe PDF
- Text
- JPEG
- PNG
- Semi-structured documents may be exported in XML or JSON format.

Proposals shall indicate the Applicant will provide data architecture documents including entity relationship diagrams documenting semantic and logical data relationships, along with a data dictionary describing datasets and data attributes. See the section entitled Metadata Standards for details. Revised documents must be provided to the City should any relevant changes occur.

4.2 Master Data Requirements

The City's master data strategy includes initiatives to provide vendors with a single source of authoritative data, and for vendor systems to in turn contribute authoritative data back to the City's enterprise data warehouses. Accordingly, the City requests the Applicant's proposal include the following:

1. Language indicating that City authoritative data shall be leveraged in the proposed solution if such data exists. City authoritative data is cataloged at https://metadata.phila.gov which must be used as a reference for this activity.
2. The Applicant's plan shall include the identification of all new datasets generated or stored in third-party information systems implemented under the scope of the proposed project. The plan must include metadata creation as per City Metadata Standards outlined in the next section.
3. Language indicating that the Applicant shall support the City as needed to meet data governance requirements including assistance with metadata creation and mentoring City Data Stewards on appropriate data usage and sensitivity.

In addition to the above, the Applicant shall provide references or case studies exhibiting integration with data warehouses developed in-house, or with other customers.

Systems integration software code developed by the Applicant or related parties is subject to RFP Section 2.4.4: Software Source Code.

4.3 Metadata Standards

To ensure appropriate use and interpretation of all vendor-supplied data in City systems, the City requires that Applicants provide the following minimum metadata documentation:

1. An overview of the dataset including its scope, purpose, and context for the intended use.
2. A detailed description of the development process for creating the data, including data sources and/or data collection methods; algorithmic, analytical, or manual transformations of the raw data; documentation of any excluded, removed, or redacted data; and any other relevant elements that contributed to the end data product.
3. Documentation of the dates when data was collected, or the timeframe represented.
4. A Data Dictionary documenting the following information for each field in the dataset:
    1. The raw field name
    2. A human-readable title for that field
    3. The type of data stored in that field (e.g., string, integer, GUID, etc.) along with any relevant details such as length, precision, geometry type, grid resolution, as applicable
    4. A complete definition of any coded values
    5. Identified primary and foreign keys (if applicable)
    6. Any other descriptive information relevant to interpreting the data such as the universe, timeframe, or exclusions specific to a given field.
    7. Additional details about geospatial data, described below.

4.4 Common Data Elements for Geospatial Data

The City has defined common data elements, defined below, for data that can be associated with a geographic location within the City. The City requires that Applicants conform to the following standards:

4.4.1 Addresses

See OIT Address Standards in Related Links, Below

All systems that process or store address data must use the City's Address Information System (AIS) for Philadelphia based address standardization, validation, or geocoding.

4.4.2 Land Records

The City has created a standard Property Identification Number (PIN) used to uniquely identify parcels, condominiums, land rights, and easements. All systems that handle land

record related data or documents shall identify property records using the City's Property Identification Number (PIN).

4.4.3 Geospatial Vector Data

Vector data consists of points, curves (lines), and polygons and derivations thereof as defined by OGC standards. Systems that store geospatial data in a Relational Database Management System (RDBMS) shall store the data according to the Open Geospatial Consortium's (OGC) standards for simple feature access. The City requires implementations of the OGC standards to follow either the Esri ST_Geometry or PostGIS Geometry specifications.

Geospatial Vector data stored outside of an RDBMS shall be stored in industry-standard formats including geojson, shapefile, or ESRI File Geodatabase.

Geospatial Vector data shall include a Coordinate Reference System (CRS) deemed appropriate for the dataset. The City requires the use of either the NAD83 or WGS84 datum. The epoch date of the chosen datum shall be documented to ensure the City can perform accurate datum transformations.

4.5 Data Protection and Retention

The Applicant will contractually agree to protect and secure the data in keeping with the City's security and all applicable regulatory requirements. This includes meeting retention requirements defined in the data owner's current Record Retention Schedule issued by the Department of Records. The buyer should seek counsel from the City Solicitor's Office, Commercial Law Unit to ensure the appropriate data protection and retention language is in the contract.

5 Roles and Responsibilities

Writing	Implementing	Using	Auditing
OIT Enterprise Architecture	IT Leadership	City staff in a procurement role, Software Engineers, Applicants and Implementers, Staff writing solicitations for systems will store City data	IT Leadership

6 Compliance

If OIT, through its process for reviewing IT implementations, finds a system to be non-compliant, OIT reserves the right to:

- temporarily halt or permanently cancel implementations.
- remove associated systems and assets from the City's network.
- order hosting and SaaS providers to quarantine or shut down associated assets.
- suspend any accounts associated with the system.
- perform a security review or forensic analysis on the system.
- take further action as needed.

Personnel that violate this policy may be subject to disciplinary action, up to and including, termination of employment, in accordance with the disciplinary policies of his or her agency and, for personnel represented by the Fraternal Order of Police, International Association of Fire Fighters, District Council 47 or District Council 33, the terms of the applicable collective bargaining agreement.

If a City contractor or third party user knowingly or negligently commits or permits a material violation of this policy, the City may terminate the contract in accordance with its terms, and/or terminate the contractor's or third party user's access to City information systems and information, in addition to any legal or remedial actions the City may take to enforce and protect its interests.

7 Guidance

Reserved

8 Waivers

Waivers may be requested from the Compliance Office by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The Compliance Office will coordinate with the authorizing bodies within OIT to issue a decision on a waiver for sufficient reasons exercising judgment in the best interests of the City.

The Compliance Office shall maintain the central repository of all waivers.

9 Definitions

Terms defined in this standard shall have the meanings in this standard that are here provided. Terms not defined in this standard shall have the meanings contained in City Policies and Standards Glossary of Terms.

10 Authority

City of Philadelphia Executive Order No. 12-11

11 Related Links

OIT Address Standard

https://phila.city/display/citygeo/Addressing+Standards

12 Change Log

Version No.	Date	Author	Description
1.0	8/26/2020	Regis Shogan	Initial Version

13 Approval

By direction of the Chief Operating Officer:

(Signed original copy on file)

_____ _____

Sandra Carter Date

Chief Operating Officer

CITY OF PHILADELPHIA ADDRESSING STANDARDS

Prepared by the Office of Innovation and Technology in coordination and cooperation with the Office of Property Data

v.06.26.2017

GOALS

These standards are consistent with recommendations prepared for Office of Property Data and align with US Postal Service (USPS) and forthcoming Next Generation E-911 National Emergency Number Association (NENA) guidelines.

The standards should be adopted for use within all database systems, applications, or tables prepared by City departments or vendors.

ALIGNMENT AND INTEROPERABILITY WITH EXISTING NATIONAL STANDARDS

- The City will use the USPS Publication 28 for address standards whenever possible.
- The Next Generation E-911 NENA standards for addressing will be adopted to the extent possible once they are published.

GOVERNANCE

- This City has full rights to determine the street names and provide the street name to USPS.
- AIS (Address Information System) was created and is maintained by the Office of Innovation and Technology (OIT) to standardize and resolve variations of address for lookup and geographic reference across city systems.
- AIS has a component, Passyunk, that is the de facto standardizer and parser for City addresses. Departments and vendors can use this application to parse and standardize addresses according to standards set by the City (see below).
- First line addresses (the house number and street name minus city, state, ZIP Code values) can be stored in tables using either single field or parsed out into the individual components described below.
- Direct questions on this standard to the Office of Innovation and Technology at maps@phila.gov Subject line: City Address Standards

ADDRESS FIELD COMPONENTS

COMPONENT	FIELD TYPE	EXMPLE: 1234B 1/2 E Independence Mall S Ste 12A	NOTES
Address	char(12)	1234B 1/2	Cannot be a zero, no leading zeros
Address Number	num	1234	Cannot be zero
Address Suffix	char	B	Values that refer to property types should instead be in the unit designator field R(REAR), S(SIDE)
Address Fraction	char(3)	1/2	Exist in Philadelphia
Street Pre Direction	char(4)	E	N,S,E,W City doesn't have NE, SE,NW, SW
Street Name		INDEPENDENCE	Required
Street Suffix	char(4)	MALL	USPS standards. i.e. AVE not AV
Street Post Direction	char(2)	S	N,S,E,W City doesn't have NE, SE,NW, SW. The City only has 300 addresses with a post direction. Use should be deprecated if possible
Secondary Unit Designators	char(10)	STE	USPS standards. Avoid # symbol whenever possible
Secondary Unit Number	char(10)	12A	Optional
City		Philadelphia	Not used if City only address list
State	char(PA)	PA	Not used if City only address list
ZIP Code	char(5)	01234	Optional if City only address list
Zip4	char(4)	0123	Optional if City only address list

CountyFips	char(5)	42101	Optional
Status	Char(1)	A	Optional: **A**ctive, **R**etired, **T**emporary, **P**rovisional
Status Date	Date	12/20/2016	Optional

Hyphenated ranged addresses exist where tax lot consolidations have occurred. This condition exists in addresses generated by Office of Property Assessment (OPA). For hyphenated addresses, use the same Address Number component as follows. Additional fields may be used optionally

COMPONENT	**FIELD TYPE**	**EXMPLE:** 1201-05 S 58th St	**NOTES**
Address	char(12)	1201-05	Use the hyphen with no spaces between values.
Address Number Low	num	1201	Cannot be zero
Address Number High	num	1205	Optional. In OPA documentation, this is called HOUSE EXTENSION

SUPPLIMENTAL INFORMATION

1. The City has about 30,000 ranged address numbers. The format looks like this -**1201-03** S 58TH ST. This is unique to Philadelphia and will make any enterprise application development more difficult and expensive. (NYC has hyphenated addresses that have been adopted by USPS, but function differently)

2. Many datasets including Office of Property Assessment (OPA) do not have Secondary Unit Designator. They only have the Secondary Unit Number. Therefore, the default value is a hashtag "#". The Address Unit Designator must be added to all city address datasets so that the correct APT, UNIT, STE, etc., is used. These values will align with what USPS has. It is understood that buildings do not always have the same standards for this however the City and USPS should be aligned.

3. The (address) Suffix/Suff fields in OPA and Department of Records (DOR) databases are problematic to matching or geocoding operations of aggregated data from these sources as they are unique to each agency's address recording operations. See Appendices A and B.

   Address suffixes should be used for specific postal address designations that generally have an alpha character at the end of the numeric address number: 1234A Market St, 1234B Market St.

   The OPA and DOR versions of these fields are a mix values that don't match postal standards and in many cases refer to types of ownership

   a. The value '2' indicates that ' 1/2' is the address number suffix.

   b. R = REAR. Should be Secondary Unit Designator?

   c. A = Air Rights, S = Subterranean, M = Multiple, L = Leasehold, E = Encroachment, P = Parking... These are not address values and should have their own field

4. No leading zeros in street names: 1317 N **02ND** ST should be 1317 N **2ND** ST

5. Single digit range numbers should have a leading zero: **1201-3** S 58TH ST should be **1201-03** S 58TH ST

6. Address number fractions in ranged addresses need to be cleaned up and not allowed **909 1/2-11** S 9TH ST. There are 6 cases known in the city.

7. The OPA database [as of this date of the document] has a constraint on the length of street names. This affects long street names that have been abbreviated: BEN FRANKLIN PKWY, CHRIS COLUMBUS BLV.

8. Per USPS standards, the word **SAINT** should always be spelled out, not abbreviated to **ST**.

9. Per USPS standards, the word **MOUNT** should always be spelled out, not abbreviated to **MT**.

10. Per USPS standards, abbreviations should not be used in Street Names: POQUESSING **CRK** DR, wrong. POQUESSING **CREEK** DR, correct.

11. Per USPS standards, pre-directions are always abbreviated: N, E, S, W. **WEST** SOUTH ST, wrong. **W** SOUTH ST, correct. **SOUTH** ST - correct.

12. Per USPS standards, address suffix always uses the official USPS abbreviations: POQUESSING CREEK **DRIVE**, wrong. POQUESSING CREEK **DR**, correct.

13. There should be no space after MC in street names: **MC CALLUM** ST, wrong**. MCCALLUM** ST, correct.

14. The city only has 300 addresses with a post direction. Use should be deprecated, if possible.

15. County, State, and Local Highways. Not all roads in Philadelphia exist solely in Philadelphia. There is a public safety need to standardize the names of roads that cross county and state boundaries. Many of these roads do not have addresses such as Interstate 95. They still need standardized names for E-911 routing, E-911 addressing, crash reporting, etc.

16. Not all addresses will have corresponding Centerline Streets. Need to handle these exceptions: GARRISON CT, 78 S PIER, ONE PENN CENTER

17. The Street Centerline Alias table should be cleaned up to only contain Aliases and no Standardizations.

    a. Chris Columbus Ave -> Christopher Columbus Ave = **Standardization**
    b. Delaware Ave -> Christopher Columbus Ave = **Alias**

SUPPLEMENTAL DOCUMENTATION

City of Philadelphia Street Name Issues *August 10th 2016*

List of street name variations between USPS, Street Centerlines, and OPA

OPA Address Standardization Issues *August 2016 CD*

List of all the variations between the Passyunk parser and OPA addresses

Street Name Variations *May 2016*

Slide deck of Street Name variations across systems and street signs.

APPENDIX A – OFFICE OF PROPERTY ASSESSMENT SUFFIX FIELD

FROM OPA PROPERTY CD DATA DICTIONARY – 2016 CERTIFIED VALUES

PAGE #4 - SUFFIX FIELD

This is an extension of the address. In past years, because of improper planning, no space may have been left between addresses or because the width of the lot was narrow, an address with ½ was created. This is no longer permitted.

The following are the only allowable codes for suffix:

2 - to indicate ½ in address (529)
R - to indicate Rear in address (2,111)
A - to indicate Air Rights (150)
S - to indicate Subterranean Rights (55)
M - to indicate Air Rights and Subterranean Rights on a given property. (0)
E – Encroachment (1)
L - Leasehold (34)

A specific location with multiple properties in the rear will be designated by using the unit number, not the suffix. That is, a frontage property with three properties in the rear would have R1, R2 R3 in the unit number. If there are multiple Air Rights (that is the splitting of the fee simple estate on a vertical basis) they would be expressed as A-1, A-2, A-3 etc.

APPENDIX B – DEPARTMENT OF RECORDS DEED PARCELS SUF(SUFFIX) FIELD

DEPT. OF RECORDS DEED PARCEL DATABASE DOMAINS FOR SUF(SUFFIX) FIELD

Code	Description
F	Front
R	Rear
2	1/2
A	Air Rights
S	Subterranean Rights
M	Mixed (Sub and Air)
P	Parking
G	Garage
B	TBD01
C	TBD02
D	TBD03
L	TBD04
Q	TBD05
0	TBD06
1	TBD07
3	TBD08
4	TBD09
5	TBD10
6	TGD11

Office of
Innovation & Technology

General Technical Standards

SOP No:	SOP Type:	Effective Date:	Review Cycle:	Version:
1003	Standard	12/1/2022	Annual	1.6
Category:	Originating Unit(s):	Contact:		Supersedes:
Configuration Management	Enterprise Architecture	Director of Enterprise Architecture		General Technical Standards v.1.5

Contents

1 Purpose 2
2 Scope 2
3 Policy 2
4 Standards 2
5 Roles and Responsibilities 13
6 Compliance 13
7 Guidance 14
8 Waivers 14
9 Definitions 14
10 Authority 14
11 Related Links 14
12 Change Log 15
13 Approval 16

1 Purpose

The City's standard non-functional requirements for IT systems ensure that information systems are resilient and secure so that the City's information is safeguarded, and its staff can continue operations (as supported by IT systems) in the event of a disaster.

2 Scope

All city systems are in scope to be reviewed for compliance with this standard.

3 Policy

Reserved

4 Standards

The non-functional requirements listed below must be included in the requirements sections of documents that specify other system or business requirements. These documents include RFX's.

These requirements must also be adhered by vendors who are developing software for the City, system implementors, and City staff who are developing software for the City.

4.1 City Standard Non-Functional Requirements

All systems and applications must meet the following "non-Functional" requirements:

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Standard Operating System Compatibility	If the system is server-based, it must be compatible with the latest stable release of Microsoft Windows Server as defined by Microsoft, or an approved Linux distribution (currently Centos 7 and Ubuntu 18.04). If the system has a thick client, it must be compatible with the latest stable release of Microsoft Windows and Mac OS.	Yes	Yes	No	Yes, but prefer containers or serverless
Standard Database Compatibility	If a database is deployed on-premises or in a City-owned cloud environment, it must be compatible with the latest stable release of Microsoft SQL Server, PostgreSQL, or Oracle.	Yes	Yes	No	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Monitoring	The system has the ability to be monitored to provide metrics that can prevent outages and must provide immediate alerts in case of an outage in any system component. Alerting must be interoperable with third-party software (e.g. Pager Duty) via webhooks.	Yes	Yes	Covered by SLA	Yes
Browser Support	The system has been tested to work with the latest versions of popular web browsers, including mobile device browsers.	Yes	Yes	Yes	Yes
Tested	The system has a documented test plan and functional testing is conducted on every update, and has full test suite (smoke, integration, etc.) performed on every release. The system must have a dedicated test environment where all testing occurs.	Yes	Yes	Covered by SLA	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Web-Based APIs	The system's components communicate via web-based APIs wherever possible. The system's business data must preferably be available via a secure API call. APIs should be authenticated and use a role-based authentication mechanism. APIs should be versioned, and as new versions are released adequate time must be given for conversion before older versions are retired.	Yes	Yes	Yes	Yes
Secure	The City expects hosting providers to be able to produce a clean SOC2 for non-financial data. The City's security policies are based on NIST 800-53 Rev 4. The system must pass a penetration test to the City's satisfaction, be monitored for security events by the system owner, and ISG must be notified of any malignant events.	Yes	Yes	Yes	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Authentication	**For City Users**: The system supports authentication using SAML 2.0 or OAuth 2.0 – OpenID Connect via Microsoft Azure Active Directory. **For External Users**: The system supports authentication using SAML 2.0 or OAuth 2.0 - OpenID Connect, via the City's login.phila.gov platform. The system should use login.phila.gov if the solution includes public login.	Yes	Yes	Yes	Yes
Multifactor Authentication	The system provides Multi-factor authentication as per the City MFA Policy.	Yes	Yes	Yes	Yes
Access Control	Access to data and administrative functions is segmented based on a user's role. Administrative privileges are just-in-time, session based, or assigned to dedicated privileged account(s)	Yes	Yes	Yes	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Logging	Application and server logs are searchable, accessible, and stored in a discrete fault-tolerant location.	Yes	Yes	No	Yes
Disaster Recovery	The system can be recovered within the Recovery Time Objective and to a Recovery Point defined by the business stakeholders.	No, best effort applies	Yes	Yes	Yes
Web Accessibility	User interfaces meet WCAG AA 2.1 Standards. https://www.w3.org/TR/WCAG21/	Internal: Recommended Public Facing: Yes	Internal: Recommended Public Facing: Yes	Internal: Recommended Public Facing: Yes	Yes
Localization	Software should have localization features for the following recommended languages: Spanish, Simplified Chinese, Vietnamese, Portuguese, Russian, French, Arabic, Haitian Creole, Swahili.	Internal: Recommended Public Facing: Yes	Internal: Recommended Public Facing: Yes	Internal: Recommended Public Facing: Yes	Internal: Recommended Public Facing: Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
User Experience	The system's ornamentation, including branding, color schemes, look-and-feel, and navigation schemes et. al. should to adhere to City Digital Standards. standards.phila.gov	Yes	Yes	Yes	Yes
System documentation	Documentation for administrators and end-users is provided. Administrator documentation includes instructions for deploying, maintaining, and auditing the system for security events such as unauthorized access.	Yes	No	No	Yes
Interface documentation	Documentation must clearly identify integrations, including data sets transferred, frequency and schedules of flows, mechanisms and protocols of transfer, and API services used and offered to others	Yes	Yes	Yes	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Data documentation	The solution design should identify data managed by the solution that is considered 'system-of-record', data that is duplicated from other sources and offered to others as 'authoritative sources', and data that integrates with any master data management processes.	Yes	Yes	Yes	Yes
User Analytics	The software must provide web page use analytics, such as user interactions, time spent on a page, and site referrals, etc., or otherwise be able to integrate with an analytics package.	Yes	Yes	Yes	Yes
SLA	The system must be available at least 99.9% of the time, or higher if there is a business need. Deploying updates to the system should not cause downtime outside of those scheduled and documented as part of a Service Level Agreement.	No, best effort	Yes	Yes	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Encryption	Data is encrypted in transit and at rest using contemporary standards such as TLS and AES. For appropriate regulated data (e.g. CJIS) the City should have the ability to manage the encryption keys.	Yes	Yes	Yes	Yes
Remote Worker Friendly	Users should not have to log on to the City's VPN in order to establish a secure connection to an application. The system should be able to operate on internal networks *and* securely over the Internet. If the above is not possible, the system should be offered on Virtual Desktop Infrastructure (VDI) that has secure communications with the system and is segmented appropriately from the end users' PC.	Yes	Yes	Yes	Yes

		Required For:			
Requirement	**Description**	**City Hosted COTS**	**Vendor Managed /Hosted**	**Software as a Service**	**Custom App**
Shared Services	The system must use applicable OIT shared services to avoid duplicating capabilities. These include, but are not limited to: • OIT Middleware such as DataBridge and Software AG Webmethods • Active Directory • Monitoring (Solarwinds, CloudWatch) • Enterprise VxRail or AWS hosting environments • Enterprise Database environment A full list of shared services is available via hyperlink at the end of this document and can be exported in MS Word format to share externally as needed.	Yes	Yes	Yes	Yes

Additional requirements for custom apps:	
Deployable	At least 2 City staff members must know how to deploy the application. The deployment process is documented.
CI / CD	The application has CI and CD in place.
Version Control	• Source code for the application is uploaded to version control environment (Github). • The app has a supported branching strategy.
Mobile	• Either a fully native version of the app must be developed or a fully responsive version. • Applications must be developed "mobile first."

Developer Documentation	• Documentation exists and covers at least the following:
	  ○ how to develop the app locally.
	  ○ how to deploy the app.
	  ○ how to debug the app.

Repository	• City Github account • City NPM account • City Terraform Enterprise account

5 Roles and Responsibilities

Writing	Implementing	Using	Auditing
OIT Enterprise Architecture OIT Software Engineering	IT Leadership	City staff in a Procurement role Software Engineers Vendors and Implementors Staff writing RFIs and RFPs	IT Leadership

All City staff responsible for decision-making regarding procuring or developing information systems are responsible for implementing this policy as criteria in their work — including RFP documents, vendor system selection, system assessments/reviews, and system design.

6 Compliance

If OIT, through its process for reviewing IT implementations, finds a system to be non-compliant, OIT reserves the right to:

- temporarily halt or permanently cancel implementations
- remove associated systems and assets from the City's network
- order hosting and SaaS providers to quarantine or shut down associated assets
- suspend any accounts associated with the system
- perform a security review or forensic analysis on the system, and/or
- take further action as needed.

Personnel that violate this Policy may be subject to disciplinary action, up to and including, termination of employment, in accordance with the disciplinary policies of his or her agency and, for personnel represented by the Fraternal Order of Police, International Association of Fire Fighters, District Council 47 or District Council 33, the terms of the applicable collective bargaining agreement.

If a City contractor or third party user knowingly or negligently commits or permits a material violation of this policy, the City may terminate the contract in accordance with its terms, and/or terminate the contractor's or third party user's access to City information

systems and information, in addition to any legal or remedial actions the City may take to enforce and protect its interests.

7 Guidance

The table of City Standard Non-functional Requirements must be used as an RFX Appendix.

The list of OIT Shared services is provided as an example and must be changed depending on the type of solution sought. For example, a GIS based solution must list ArcGIS. Refer to OIT Shared Services in the Additional Resources section below for a full list.

8 Waivers

Waivers may be requested from the Compliance Office by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The Compliance Office will coordinate with the authorizing bodies within OIT to issue a decision on a waiver for sufficient reasons exercising judgment in the best interests of the City.

The Compliance Office shall maintain the central repository of all waivers.

9 Definitions

Terms defined in this policy shall have the meanings in this policy that are here provided. Terms not defined in this policy shall have the meanings contained in City Policies and Standards Glossary of Terms.

10 Authority

City of Philadelphia Executive Order no. 12-11

11 Related Links

OIT Shared Services: https://phila.city/display/ea/OIT+Shared+Services

City Digital Standards: standards.phila.gov

City of Philadelphia Web Accessibility Policy

WCAG AA 2.1 Standards: https://www.w3.org/TR/WCAG21/

12 Change Log

Version No.	Date	Author	Description
1.0	8/26/2020	Regis Shogan	Initial Version
1.1	1/28/2021	Regis Shogan	Added Remote Worker Friendly Requirement
1.2	10/7/2021	Regis Shogan	Annual review
1.3	12/1/2021	Dan Lopez & Regis Shogan	Add External User Authentication. Update Shared Services examples
1.4	1/12/2022	Regis Shogan	Add Encryption
1.5	1/13/2022	Regis Shogan	Add interface documentation and data documentation. Generic Updates
1.6	4/7/2022	Regis Shogan	Added matrix for internal / vendor managed / SaaS / Custom

13 Approval

By direction of the Chief Operating Officer:

(Signed original copy on file)

Sandra Carter

Chief Operating Officer

Date

CITY OF PHILADELPHIA DIGITAL STANDARDS

http://standards.phila.gov/

Philadelphia's digital standards provide the design, code, and content guidelines for City websites. These standards were created by the Office of Open Data and Digital Transformation for people who are designing, creating, and writing for the City of Philadelphia. Standards allow as many people as possible to access City information. Standards also help outside vendors and individual departments, offices, commissions, and agencies create a consistent identity for the City of Philadelphia.

These standards are divided into guides for:

- **Design and Development:** the visual branding elements and tools that define how City websites should look and function.
- **Content:** all the information you need to write for City websites.
- **Analytics:** as part of the City's commitment to open data, we employ a Unified Web Analytics Strategy and have included the necessary code for employing it.

Please review the guides and technical details at http://standards.phila.gov/

CITY OF PHILADELPHIA

WEB CONTENT ACCESSIBILITY STANDARDS

All sites produced by vendors for the City, regardless of the hosting environment, shall conform to the WCAG 2.1 AA Accessibility Guidelines. Click Link to view

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 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 the 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.