Information Technology Standard

City of Phoenix

Domain: Business	Number: s1.20	Standard Title: Cloud Computing Security Standard	
Original Approval	03/23/2012	**Last Updated/Approved**	03/23/2012
Compliance Date	03/23/2012	**Last Reviewed**	11/2/2018
Owner	Information Security and Privacy Office		
Approvals	Chief Information Officer		

I. Purpose – Summary of Intent

This document establishes standards and guidelines for the selection of Cloud Computing Service Providers and/or cloud delivered services/solutions within the City of Phoenix. A cloud service should be considered for all new reportable and non-reportable IT projects whenever a feasible and cost-effective solution is available that meets the City/Department requirements, and provides the required level of security, performance and availability consistent with the City Administration Regulation and Information Security Standards.

This document also defines required security safeguards to protect the confidentiality, integrity, and availability of City information and systems when conducting City business using cloud computing. Appropriate security safeguards are based in part on the classification of the information being handled. Questions about information classification should be directed to Information Technology Services, Information Security and Privacy Office. Reference: s1.9. Information Classification.

II. Definitions – Terms Specific to the Standard

City Business – Work performed that has a direct relation to the City's operation and activities. For the purposes of this standard, City business includes any work performed where non-transient public records may be created, transmitted, or stored. Reference: City of Phoenix Public Records Request Handbook.

Cloud Computing – The National Institute of Standards and Technology (NIST) defines Cloud Computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud Service Provider (CSP) – A cloud service provider is a company that offers some component of cloud computing -- typically infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS) -- to other businesses or individuals.

Confidential Data – As defined in A.R. 1.90, confidential data includes, but is not limited to the following: Criminal Justice Information (CJI); Payment Card Information (PCI); Protected Critical Infrastructure Information (PCII); Protected Health Information (PHI); Personal Identifying Information (PII), and Restricted City Information (RCI).

FedRAMP – The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

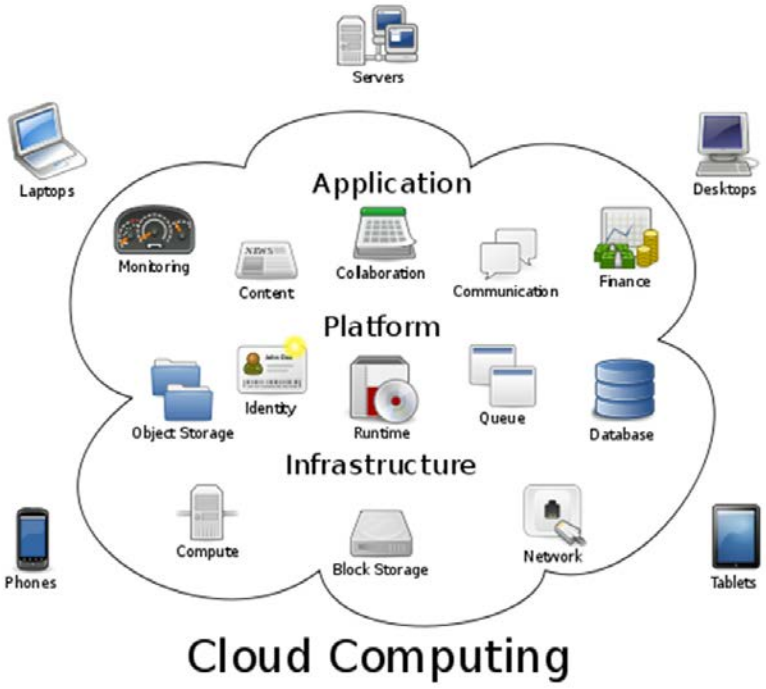
Infrastructure-as-a-Service (IaaS) – The capability provided to an organization to provision processing, storage, networks and other fundamental computing resources along with the ability to deploy and run arbitrary software, which can include operating systems and applications. The organization does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).

Platform-as-a-Service (PaaS) – The capability provided to an organization to deploy onto a cloud infrastructure using organization owned applications. The organization does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Software-as-a-Service (SaaS) – The capability provided to an organization to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The organization does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Subscription Based Cloud Services – Contracted cloud services that are provided through a subscription plan. Instead of paying upfront for a perpetual license (and periodic maintenance fees where applicable), the user will have to submit regular payments every month or every year in order to use the software. SaaS is commonly provided through a subscription plan.

Domain:	Number:	Standard Title:
Security	s1.20	Cloud Computing Security Standard



Cloud computing encompasses applications, platforms, and infrastructure.

III. Applicability

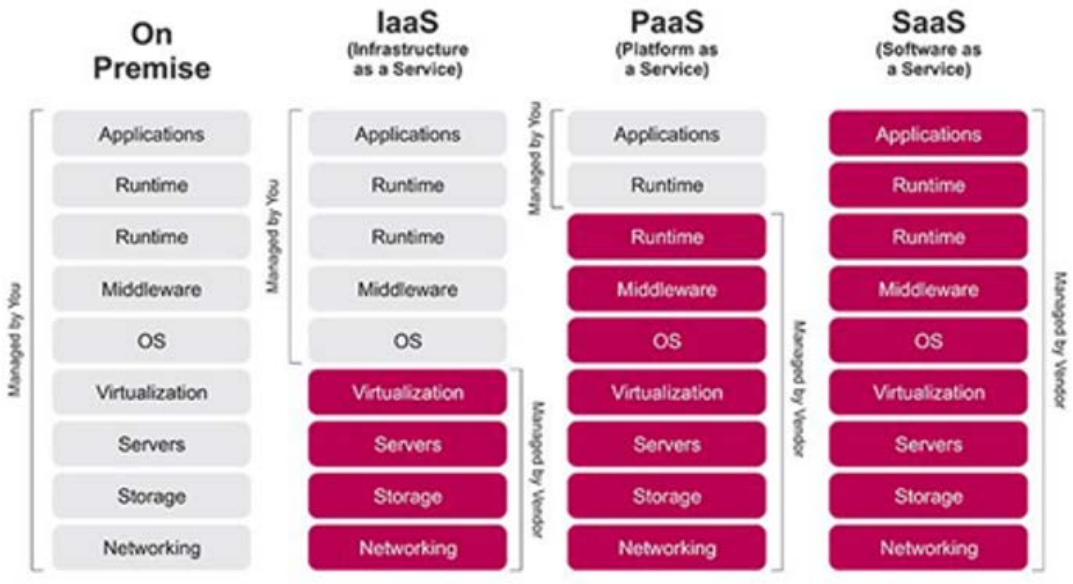
This standard applies to all City of Phoenix personnel including City employees, business partners, contractors, temporary workers, volunteers, elected officials, and those in appointed positions. This standard supersedes all previous versions of this standard.

IV. Roles and Responsibilities

Department heads are responsible and accountable for assuring the confidentiality, integrity, and availability of their department's information, no matter where it resides.

Standard Cloud Computing type descriptions and responsibilities diagram are shown below:

Domain:	Number:	Standard Title:
Security	s1.20	Cloud Computing Security Standard



V. Cloud Computing Policy

New Cloud Service Implementations

City Departments must complete the Information Security Risk Assessment Questionnaire section of the Business Information Request Form (BIRF) prior to contracting with a Cloud Service Provider (CSP). This assessment is used to validate the use of cloud services is technically and administratively viable and to ensure that adequate protection measures are taken concerning City data, liability, security, and other City requirements.

Department Procurement Officers should work with the requestors and CSP to complete the questionnaire. Completed questionnaires will be uploaded as part of the online BIRF process and forwarded to the Information Security and Privacy Office (ISPO) for review.

Depending on the scope, ISPO will determine whether an IT Security review is needed, advise on alternative solution pathways, if relevant, and/or provide other guidance, as applicable.

Regardless of the hosting site, City data that is stored on third-party CSP hosted sites must adhere to City information security Administrative Regulations and information security standards to ensure that they are commensurate with the classification of any data stored in the cloud.

Existing Cloud Service Implementations

When requested, City Departments will provide information to ITS regarding existing cloud service implementations, including those in use prior to this policy revision if still active. ITS will collect information on all cloud services used across the City to review issues related to security, bandwidth, and interoperability. Building and maintaining this Citywide inventory of cloud services will be critical to ensuring that the City is prepared to prevent and respond to potential security threats or compromises in a timely manner. In the event ITS identifies potential security

risks associated with existing cloud service implementations, ITS will work with affected departments to eliminate or mitigate the risks.

VI. Cloud Computing General Requirements

Listed below are general requirements for all City information processed, stored, or transmitted via cloud computing.

1. **FedRAMP**. Whenever available, FedRAMP certified cloud solutions should be selected over non-FedRAMP certified cloud solutions.

2. **Records Management**. City staff electing to use cloud computing services must ensure they are in compliance with all records retention and eDiscovery policies and schedules. Reference: A.R. 1.61 Records Management Program.

3. **U.S. Based.** CSP will store City confidential data (CJI, PCI, PCII, PHI, PII, RCI) within a data center located within the Continental US - including backups. If a cloud provider is selected that is not U.S. based, a waiver is required, and the Law Department in consultation with ISPO should thoroughly vet the cloud provider prior to use. Depending on the sensitivity of the data, a certified government cloud (Microsoft Azure, Amazon AWS GovCloud, etc.) may be required.

4. **Third-Party Assessments.** CSP will provide the City with results of a third-party external Information Security assessment (SAS-70, SSAE-16/18, penetration test, vulnerability assessment, etc.) or other Statement of Controls (SOC) reports.

5. **Personal Cloud Services**. Personal cloud services accounts may not be used for the storage, manipulation or exchange of City-related communications or City-owned data (e.g. Dropbox (free version); personal OneDrive; or personal Gmail accounts).

6. **Subscription Based Cloud Services**. Subscription based cloud services which are limited in size and scope and cannot be adequately addressed by other means, may be approved following a risk assessment by ISPO. A waiver may need to be provided outlining compensating controls. Departments are still required to submit the Information Security Risk Assessment Questionnaire section of the BIRF.

VII. Cloud Computing Data Requirements

1. Terms and Conditions. Cloud providers shall include terms to abide by the duties of confidentiality in the Terms and Conditions and/or Privacy Policy, thereby ensuring that the online data storage provider has an enforceable obligation to preserve users' confidentiality and security of user data.

2. Data Classification. Based on data classification ensure compliance with relevant security provisions including Internal Revenue Service (IRS) Publication 1075, Social Security Administration (SSA) Electronic Information Exchange Security Requirements, Payment Card Industry Data Security Standard (PCI DSS) including the PCI DSS Cloud Computing Guidelines, Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Health Information Technology for Economic and Clinical Health (HITECH) Act, and Criminal Justice

Information Services (CJIS) Security Policy. FIPS 140-2 is recommended for encryption compliant standards, NIST 800-175B.

3. **Contractual Controls.** The City must have a contract or agreement in place with the cloud computing provider(s) that is approved by the Law Department and contains provisions that provide for confidentiality and data security safeguards for information in the cloud computing provider's custody, Discovery and Destruction of data and NDA.

4. **Certifications.** Cloud providers should host on reputable cloud services that have obtained one of the following certifications or met similar indicia. Certifications are used to gain confidence and place trust in a service organization's systems.

   a) Type 2 SOC. A Service Organization Controls ("SOC") Type 2 report evaluates an organization's information systems as they relate to security, availability, processing integrity, confidentiality, and privacy of a system.

   b) ISO 27001. ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it provides a framework of how to manage information security in a company. The main philosophy of ISO 27001 is based on managing risks: find out where the risks are, and then systematically treat them.

   c) ISO 27018. ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of Personally Identifiable Information ("PII") which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

5. **Data Retention Policy**
   Cloud providers will follow city data retention policy. The Cloud provider should meet or exceed the data retention policy of the City in pursuant of A.R. 1.61. Additionally, the Cloud providers should take reasonable steps to ensure that when data is deleted from the cloud provider's environment, the cloud provider has measures in place to ensure the data is no longer available to any entity.

6. **Data Ownership**
   All data is owned exclusively by the City Department contracting with the CSP and cannot be used by the CSP for any purpose other than the services provided to the customer. Additionally, the CSP should not be able to remove metadata and is given no right to use City data for any purpose other than serving the City as a customer.

7. **Demands for Data - Must Be Authorized By the City**
   Cloud providers must notify the City of demands for their information by 3rd parties as soon as possible, unless the provider is specifically prohibited from doing so by law.

8. **Data Breach**
   The CSP should notify the City contracting Department as soon as reasonably practicable, but not more than seventy-two (72) hours following the Contractor's discovery of any breach of the security of customer data if personal or health care information was, or is reasonably believed to have been, acquired or accessed by an unauthorized person. The CSP should

also notify the City Attorney and the Chief Information Security Officer.

CSP shall agree to reimburse the City for any costs incurred by the City to investigate and respond to potential breaches of this data, including, where applicable, the cost of notifying individuals who may be impacted by the breach, attorneys' fees, and for any monetary damages or penalties the City is assessed. In case of a breach or critical breach of the City's information, it will be the City, not the CSP that will inform any and all individuals affected by any such breach. Only upon prior written consent of the City, or at the specific direction of the City, will the CSP notify individuals affected by a breach or critical breach of the City's information.

The CSP shall maintain an effective incident response and mitigation capability for security and privacy incidents in accordance with industry best practices.

VII. Cloud Computing Security Requirements

1. Encryption

Cloud providers will be required to maintain data encryption protocols covering:

a) Data stored at rest in the data center, and
b) Data transmitted to and from the data center
c) Key management requirements including key escrow

Ensure that confidential, sensitive or personal information is encrypted in accordance with NIST 800-175B and ISO/IEC 27018, and at the necessary level of encryption for the data classification pursuant to s1.9.

Strong encryption may protect data from unauthorized access, copy, modification or other attacks to the integrity and security of the data.

2. Testing

Cloud providers should disclose if and how frequently vulnerability or penetration testing and/or ethical hacking services are being performed on their offering. Some of the testing methods are listed below:

a) **Vulnerability Scans.** A vulnerability scan is the process of identifying and quantifying security vulnerabilities in an environment. It identifies security flaws based on a database of known flaws, tests a system for the occurrence of these flaws, and provides a report of exposures and the associated level of risk for each confirmed vulnerability. Remediation of identified vulnerabilities should be based on specific timelines and severity (CVSS v2/v3, CVE, CWE).
b) **Penetration Testing**. Penetration testing is an actual internal or external attack with the intention of gaining unauthorized access to systems and the data stored within the network.
c) **Static Code Reviews.** Static analysis code testing provides an understanding of security issues within program code. It is a systematic review of the software source

code without executing the code. The main objective of this testing is to find errors in the early stages of the development cycle.

d) **Dynamic Code Reviews**. A Dynamic Code analysis relies on studying how the code behaves during execution. It monitors system memory, functional behavior, response time and overall performance of the system. The main objective of this testing is to find and fix any defects.

3. Antivirus/Antimalware Controls. CSP should have active antivirus/antimalware controls in place to protect against sophisticated cyber-criminal activity.

4. **Multifactor Authentication (MFA).** All cloud providers will provide the capability for City staff to utilize/integrate appropriate multifactor authentication with cloud services with additional control and account lockout on failed authentication. Examples could include strength of password requirements (password entropy), certificate-based protocols, and device authentication.

5. **Authorization and Access.** The CSP should enforce the following IT security best practices:
   a) **Least Privilege:** Only authorize access to the minimum amount of resources required for a function.
   b) **Separation of Duties:** Functions shall be divided between staff members to reduce the threat that one person can commit fraud undetected.
   c) **Role-Based Security:** Access control shall be based on the role a user plays in an organization.

6. Business Continuity. Where Business Continuity/Disaster Recovery (BC/DR) services are required, all agreements should establish terms for BC/DR, and the CSP must demonstrate its ability to fulfill the terms. If BC/DR is required, such requirements take precedence over the force majeure clause.

7. Exit Strategy. Cloud provider must provide City with a Cloud Exit Strategy. The exit strategy should cover a normal termination, such as that at expiration of the service agreement, and an unexpected termination, such as that due to service provider bankruptcy, exit from line of business, and/or poor performance. Strategy should state expected timely export of data as well as the format of the City's data returned through a secure channel with verification in writing by the Cloud provider that City hosted data has been thoroughly purged from its systems and database. Other aspects include addressing application dependencies on proprietary programming interfaces, system calls, and database technologies, as well as the recovery of useful metadata that may have accumulated within the cloud environment.

8. Concluding Activities
Departments should perform the following activities preceding the termination of an outsourcing contract:

- **Reaffirm Contractual Obligations.** The Department should alert the cloud provider about any relevant contractual requirements that must be observed upon termination, such as non-disclosure of certain terms of the agreement and sanitization of organizational data from storage media.

- **Eliminate Physical and Electronic Access Rights.** If any accounts and access rights to a Departments computational resources were assigned to the cloud provider as part of the service agreement, they should be revoked in a timely manner by the Department. Similarly, physical access rights of security tokens and badges issued to the cloud provider also need to be revoked, and any personal tokens and badges used for access need to be recovered.

- **Recover Organizational Resources and Data.** The Department should ensure that any resources of the Department made available to the cloud provider under the terms of the service agreement, such as software, equipment, documentation, are returned or recovered in a usable form, as well as any data, programs, scripts, etc. owned by the organization and held by the cloud provider. If the terms of service require the cloud provider to purge data, programs, backup copies, and other cloud consumer content from its environment, evidence such as system reports or logs should be obtained and verified.

VIII. Compliance Audits

The City Auditor Department may conduct periodic audits to evaluate compliance with the requirements set forth in this IT standard. The City Auditor Department may require proof of certifications and reports as needed i.e. ISO27001, SOC2 Attestation of Compliance etc. from the cloud provider.

City personnel must comply with this standard at all times. City of Phoenix reserves the right to monitor systems, electronic communications, and usage to ensure compliance.

IX. Related Policies, Standards, and Procedures

A.R. 1.61, Records Management Program
A.R. 1.63, Electronic Communications and Information Acceptable Use
A.R. 1.90, Information Privacy and Protection
A.R. 1.91, Information Privacy and Protection Supplement — Data Shared with Third Parties
b1.3 Waiver Standard
s1.9 Information Classification