# Cloud Acquisition & Management Policy

Committee on Information Technology

The City and County of San Francisco encourages the use of cloud services when cost efficiencies are available, risk mitigation strategies are in place, and the services support the City's data sharing strategy through interoperable systems.

## PURPOSE AND SCOPE

The purpose of the Cloud Acquisition & Management Policy is to ensure City departments incorporate the appropriate requirements, processes, and risk mitigation strategies in the use and procurement of cloud services. This policy encompasses the City's use of all cloud services, which includes but is not limited to: storage, software-as-a-service (SaaS), and platform-as-a-service (PaaS) products.

The requirements identified in this policy apply to all information resources operated by or for the City, and County of San Francisco and its departments, and commissions. Elected officials, employees, consultants, and vendors working on behalf of the City and County of San Francisco are required to comply with this policy.

## POLICY STATEMENT

Before the purchase or use of cloud services, the Cloud Acquisition & Management Policy requires all departments to incorporate the following procedures:

Acquisition Requirements - Conduct a formal evaluation and document the following:

- The department CIO or IT Manager must explicitly express approval before the use of any cloud service. City employees may not provision cloud products without approval from the department CIO or IT Manager and must follow the Office of Contract Administrations procurement policies.
- Departments shall use existing contracts as to maximize the City's purchasing power where appropriate.

Data Standards & Risk Mitigation

For all cloud services, departments shall:

- Conduct a risk assessment of data privacy risks with the service. Products that contain level 3-5 data should have added level of review and comply with the department's cybersecurity requirements and identity access and management rules. To classify data, department should refer to the COIT Data Classification Standard.
- Verify the City retains ownership and rights to City Data, including derivative works made from City Data and the licensing applied to the data.
- Define data retention standards for all data stored with cloud services.
- Consider the interoperability of a cloud service with the City's data and systems. Departments should prioritize products that use application programming interface (API) standards that support the City's data sharing goals.

In all instances, departments should consult with the Department of Technology on the appropriate technology strategies.

### COIT Policy Dates

Approved: March 21, 2019
Next Review Date: FY 2020-21

## ROLES AND RESPONSIBILITIES

- **Department CIO's & IT Managers** shall:
  - Review all uses of cloud services within their departments and provide approval for use where appropriate.
  - Evaluate and ensure existing cloud services maintain robust cybersecurity and continuity of operations practices (e.g. failover tests, network penetration testing, etc…)
  - Coordinate closely with the Department of Technology and the City's Cybersecurity Office to provide a comprehensive picture of the City's use of cloud products.
  - Work with department risk manager and the City's Chief Information Security Officer to conduct formal risk assessments where warranted.
  - Define data retention standards for all cloud services, and verify ownership of all City data.
  - Communicate with department employees the approval process for cloud products to ensure employees shall not self-provision cloud products without guidance.

- **Department IT Security Officers** shall:
  - Work closely with their department technology leadership to conduct risk assessments for cloud products.
  - Coordinate with the City's Chief Information Security Officer regarding appropriate risk levels and best practices.

- **Department of Technology** shall:
  - Provide information and support on selecting appropriate cloud products. The Engagement Portal will be a resource to share current cloud providers in the City.

- **City Chief Information Security Officer** shall:
  - Support risk assessments for cloud services interfacing with critical systems, and support departments as they seek to classify their data according to the Data Classification Standard.

- **Office of Contract Administration** shall:
  - Support departments to use appropriate procurement method for cloud services. The purchase of SaaS products via Tech Marketplace may only contain data level 1 and 2 data as defined by the Data Classification Standard.
  - Reference the P-648 contract template for Software-as-a-Service as appropriate.

- **The City Attorney's Office** shall:
  - Structure contracts to include provisions from this policy in the procurement of cloud services.
- **City Services Auditor** shall:
  - Periodically review department compliance with the Cloud Acquisition Policy.
  - Evaluate the application of the Data Classification Standard towards department cloud products.

## DEFINITIONS

- "City Data" includes without limitation all data collected, used, maintained, processed, stored, or generated by or on behalf of the City, including as the result of the use of the services provided by a contractor.

## COMPLIANCE

- A department may restrict access to any cloud service that fails to comply with this policy, until the requirement is met.

## REFERENCES

- COIT Data Classification Standard: https://sfcoit.org/datastandard
- COIT Citywide Cybersecurity Policy: https://sfcoit.org/cybersecurity
- Department of Technology Engagement Portal:https://sfgov1.sharepoint.com/sites/TIS/Collaborations/SitePages/Engagement%20Portal.aspx
- Office of Contract Administration Contract Template P-648: https://sfgov.org/oca/frequently-asked-questions-0

## APPENDIX A: CLOUD SERVICES DEFINITION

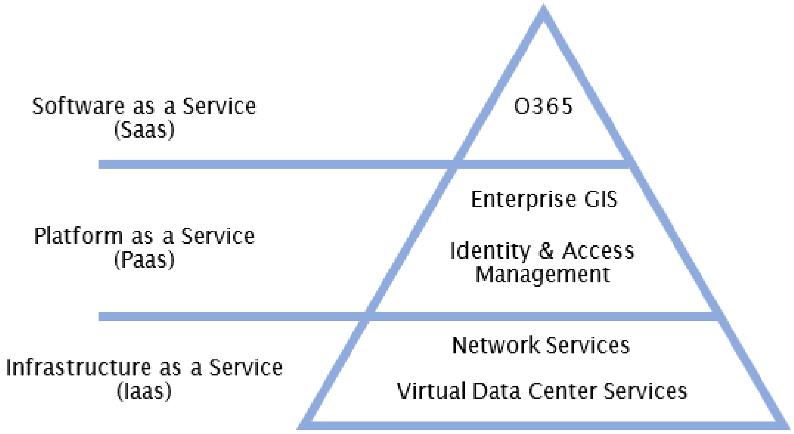
External cloud providers offer services that provide a number of potential advantages over on premise solutions, including: scalability/elasticity, the elimination or reduction of data center footprint, and hardware purchases, operating system refresh, solid security, and features such as development tools, database or middleware.

The most common cloud services are:

- ***Infrastructure as a Service (IaaS):*** IaaS provides virtualized computing resources such as processing and storage over the Internet and enables subscribers to deploy and run software. The subscriber does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications. Amazon Web Services is an example of IaaS.

- ***Platform as a Service (PaaS):*** PaaS provides subscribers with a platform by which to develop, run, and manage web applications using the provider's programming languages, libraries, services, and tools. The subscriber has control over the deployed applications. Heroku or CloudFoundry are example PaaS products.

- ***Software as a Service (SaaS):*** SaaS is a software licensing and delivery model by which software and/or applications are licensed on a subscription basis and centrally hosted by the software provider. Salesforce.com is an example of SaaS.



## APPENDIX B: SOFTWARE AS A SERVICE (SaaS) CONTRACT GUIDELINES

When negotiating services with a SaaS provider, Departments are advised that a standard SaaS contract is also available for use with the Office of Contract Administration. For SaaS products that only contain level 1 or level 2 data as defined by the Data Classification Standard, the Tech Marketplace is an option. However for all other procurements, the standard contract is an option for future negotiations. Some of the contract provisions include:

- *Availability of data* - The agreement should address the uptime the city expects through a service level agreement.
- *Sensitivity of data* - Agreements concerning data such as health information, personal identifiable information, credit card information, or whether a person is a public benefits recipient must reflect additional regulatory compliance requirements.
- *Data breach considerations and remedies* – The agreement should define the risks of and responsibility for breaches of data.
- *Online and hosting facility security* – Encryption services and physical security procedures should be documented. Certain types of data require special certification.
- *Ownership and location of data* - The vendor's employees should only access the city's data to the extent necessary to maintain the service. The use de-identified aggregate data should be carefully considered.
- *Disaster recovery and location of the primary and back up data centers* - The location of primary and backup secondary centers, including the city and state, and ensure the agreement requirements flow down to the subcontractor.
- *Limitation on Click-Wrap Disclaimer* - The agreement should state that only the written provisions of the parties' agreement apply to the city's designated users for access, not the click-wrap agreement often required to gain access to the service.
- *Records Retention Policy and Litigation Holds* - The agreement should address what the city expects the hosting provider do in the event of a litigation hold.
- *Audits* - Audits should be performed on a regular basis and a summary or copy of an SSAE 16 audit report provided to the city.
- *Termination provisions and vendor bankruptcy* - On termination or expiration of the agreement, the hosting provider should provide the city with a complete copy of the city's data in an agreed upon machine readable format within a specified timeframe, and require the hosting provider to certify in writing that it will purge all city data from the vendor's servers in a way that the data cannot be recreated.

Complete details with all standard provisions contained in the SaaS P-648 contract is available on the Office of Contract Administration's website at: https://sfgov.org/oca/frequently-asked-questions-0.