COMMONWEALTH OF VIRGINIA

Information Technology Resource Management (ITRM)

CLOUD-BASED HOSTING SERVICES FOR

IT SOLUTIONS POLICY

Virginia Information Technologies Agency (VITA)

Publication Version Control

Questions related to this publication should be directed to the Enterprise Architecture (EA) Division in VITA. EA notifies Agency Information Technology Resources (AITRs) at all state agencies, institutions and other interested parties of proposed revisions to this document.

This following table contains a history of revisions to this publication.

Version	Date	Revision Description
EA 300-01	10/15/2018	Initial
EA 300-02	01/26/2022	Revised to remove Appendix B, EO19

Identifying Changes in this Document

- See the latest entry in the revision table above.
- Vertical lines in the left margin indicate the paragraph has changes or additions.
- Specific changes in wording are noted using *strikethroughs*, italics, and underlines; *strikethroughs indicating language that was deleted*; italics only indicating new/added language; and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. ~~This text was deleted.~~ *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

Example of deleted section ~~– This section is deleted.~~

Review Process

VITA IT governance divisions provided the initial review of this publication.

Online Review

All Commonwealth agencies, stakeholders, and the public were encouraged to provide their comments through the Online Review and Comment Application (ORCA). All comments were carefully evaluated and individuals that provided comments were notified of the action taken.

Preface

Publication Designation
COV ITRM Policy EA 300-01

Subject
Technology Policy

Effective Date
October 15, 2018

Supersedes
Initial version

Scheduled Review:
One (1) year from the effective date, then every two years thereafter.

Authority
Code of Virginia, §2.2-2007 (Powers of the CIO)

*Code of Virginia § 2.2-2007.1. (*Additional duties of the CIO relating to information technology planning and budgeting)

Code of Virginia, § 2.2-2010 (Additional powers of VITA)

Code of Virginia, Chapter 20.1 of Title 2.2 (Virginia Information Technologies Agency)

Code of Virginia, § 2.2-1115 (D) (Procurement Violations)

Chapter 806 of the 2013 Acts of Assembly, § 4-5.04 (b), as amended and reenacted

Code of Virginia, § 2.2-2699.6 (Powers and duties of the ITAC)

Scope
This policy is applicable to all Executive Branch agencies and institutions of higher education (hereinafter collectively referred to as "agencies") that are responsible for the management, development, purchase and use of information technology resources in the Commonwealth of Virginia. This policy does not apply to research projects, research initiatives or instructional programs at public institutions of higher education.

Purpose
The purpose of this policy is to establish guiding principles for creating optimal business value from IT-enabled business investments at acceptable cost and risk.

General Responsibilities

Chief Information Officer of the Commonwealth (CIO)
Develops and approves statewide technical and data policies, standards and guidelines for information technology and related systems.

Virginia Information Technologies Agency (VITA)
At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts; reviewing procurement requests, agency *IT programs and* projects, budget requests and strategic plans; and when developing and managing IT related services

Information Technology Advisory Council (ITAC)
Advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Executive Branch Agencies
Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Related COV ITRM Policies, Standards, and Guidelines
Enterprise Architecture Policy (EA200-Current Version)

Enterprise Architecture Standard (EA225-Current Version)

Table of Contents

1.0 Introduction

The purpose of this policy is to provide direction on how the commonwealth should create, govern and utilize cloud-based hosting services for IT solutions. This policy applies to everyone providing and managing the provision of IT hosting services for COV IT solutions, including those not considered part of the VITA enterprise.

2.0 Glossary

As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page on the VITA website at. https://www.vita.virginia.gov/media/vitavirginiagov/it-governance/psgs/pdf/comp-ITRMGlossary-v3.1.a-2018.pdf

3.0 Cloud-based Hosting Services

Vision
The commonwealth will provide a comprehensive portfolio of cloud-based IT solution hosting services, maximize cloud readiness, enable informed hosting decision-making by agencies/customers while ensuring and maintaining the appropriate security of commonwealth data. (adopted by VITA Customer Advisory Council (CAC))

Strategy

The commonwealth will:

- Deploy cloud-based IT solution hosting services integrated with traditional and other hosting services
- Create COV ITRM standards to support this policy, vision, and strategy
- Apply governance to all IT hosting services while ensuring vulnerabilities, risks, and impacts to business operations are weighed against the advantages of adopting cloud-based hosting services for specific agency/customer IT solutions

Agencies/customers will:

- Evaluate all existing and new IT solutions for cloud readiness as defined by COV policies and standards
- Determine the future state for all existing IT solutions
- Develop business cases to determine if current IT solutions that could be made cloud ready should be migrated to cloud-based services (private, community, public, and/or hybrid)
- Ensure all new IT solutions will either be cloud ready, or will have documented and approved business/technical exceptions
- Utilize cloud-based services for all cloud ready IT (new or existing) solutions or have a documented business rationale for not using those services

Objectives

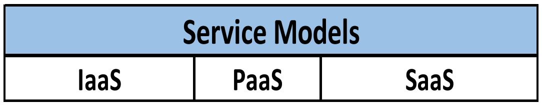
1. **Framework –** Publish COV definitions of cloud computing and establish an IT solution service hosting framework that includes integration of cloud-based with non-cloud-based hosting services
2. **Services –** Select, implement, and integrate cloud-based hosting services needed for IT solutions
3. **Suppliers –** Define NIST compliant cloud-based hosting supplier service requirements and select the suppliers to provide needed services
4. **Agencies/customers –** Establish and implement a methodology for determining which cloud-based hosting services can and should be consumed for agency IT solutions
5. **Governance –** Define and implement governance processes for cloud-based hosting services

Appendix A: Definitions

The NIST framework is composed of three service models, four deployment models, and five essential characteristics. The following definitions are from: *The NIST Definition of Cloud Computing; 800-145; September 2011.*

Cloud computing is a model for enabling ubiquitous, 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.

Three Service Models



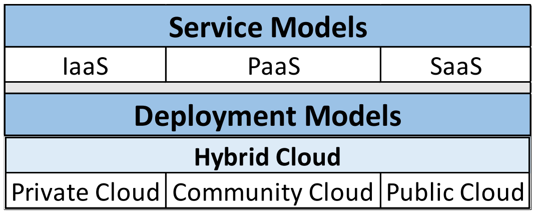
Service Models		
IaaS	PaaS	SaaS

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

Platform as a Service (PaaS) - the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer 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 configuration settings for the application-hosting environment.

Software as a Service (SaaS) - the capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer 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.

Four Deployment models



Service Models		
IaaS	PaaS	SaaS
Deployment Models		
Hybrid Cloud		
Private Cloud	Community Cloud	Public Cloud

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Private cloud options include: (Microsoft Cloud Services Foundation Reference Model (CSFRM)

- ***Self-hosted Private Cloud -*** a Self-hosted Private Cloud provides the benefit of architectural and operational control, utilizes the existing investment in people and equipment, and provides a dedicated on-premises environment that is internally designed, hosted, and managed.
- ***Hosted Private Cloud -*** a Hosted Private Cloud is a dedicated environment that is internally designed, externally hosted, and externally managed. It blends the benefits of controlling the service and architectural design with the benefits of datacenter outsourcing.
- ***Private Cloud Appliance -*** a Private Cloud Appliance is a dedicated environment procured from a supplier that is designed by that supplier with provider/market driven features and architectural control, is internally hosted, and externally or internally managed. It blends the benefits of using predefined functional architecture and lower deployment risk with the benefits of internal security and control.

Community cloud - the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). *The COV hybrid cloud will consist of at least one private cloud, more than one public (utility) cloud, more than one community (gov/FedRAMP)) cloud, and integration between these cloud hosting services.*

Five Essential Characteristics

On-demand self-service - a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access - capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service - cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Additional Hosting Options

Traditional – traditional hosting services include physical and virtual servers that do not meet the five NIST characteristics defined above. These services can be provided on-premise or off-premise (eGov). Implementation of a hybrid cloud model could be extended to cover these type of services within the service and management model.

Appliances - generally a separate and discrete hardware device with integrated software (firmware), specifically designed to provide a specific computing resource. These are generally "closed and sealed" – not serviceable by the owner. The hardware and software are pre-integrated and pre-configured before delivery to customer, to provide a "turn-key" solution to a particular problem. Unlike general purpose computers, appliances are generally not designed to allow the customers to change the software (including the underlying operating system), or to flexibly reconfigure the hardware.

On-premise vs. Off-premise

On-premise – a site or portion of a site (colocation) that is fully under control of the commonwealth or its delegated representatives. It may be either at a centralized COV datacenter facility, an agency datacenter/location or co-located (caged, etc.). Full control would include servers, storage, switches, the building, cooling, power, bandwidth physical security, etc.

Off-premise – any IT application hosting option that is not provided within an on-premise or colocation solution. The hosting site and environment is not under full control of the commonwealth or its designees (ex. public cloud suppliers).

A colocation (colo) - a data center facility in which a business can rent space for servers and other computing hardware. Typically, a colo provides the building, cooling, power, bandwidth and physical security while the customer provides servers and storage.

Cloud Service Broker (CSB) - an entity (real or virtual) that manages the use, performance and delivery of cloud services, in addition to enabling the negotiations and relationships between cloud providers and cloud consumers. NIST defines CSB as an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via *three primary roles including aggregation, integration and customization brokerage*.

Cloud Service Integrator (CSI) - specializes in the integration of cloud hosted services (sometimes referred to as Integration-as-a-Service). For the extended hybrid cloud model some of the IT solutions, services and data are maintained locally, while others are served remotely via multiple cloud providers.

Cloud ready/Cloud readiness: an IT solution that is either already or can be hosted on a virtual x86 server using either Linux or Windows as an operating system and there are no software licensing or data issues with the solution consuming cloud-based hosting services.

Container - a packaging format that encapsulates a set of software with its dependencies and runs in a virtual server environment with minimal OS. Therefore, it is a form of virtualization. The difference between VM's and containers is that each VM has its own full sized OS, while containers have a minimal OS.

Containerization - the encapsulation of an application in a container.