Virginia Information Technologies Agency

What Commonwealth Procurement Officers Need to Know About Commonwealth Security and Cloud Requirements for Solicitations and Contracts

Compliance with Commonwealth Security and Cloud Requirements

§ 2.2-2009 of the *Code of Virginia* mandates that the Chief Information Officer (CIO) is responsible for the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, standards, and guidelines shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies.

Further, it requires that any contract for information technology entered into by the Commonwealth's executive, legislative, and judicial branches and independent agencies require compliance with applicable federal laws and regulations pertaining to information security and privacy. While agencies are required to comply with all security policies, standards and guidelines (PSGs), Security Standard SEC525-02 provides agency compliance requirements for non-CESC hosted cloud solutions. These PSGs are located at this URL: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

In addition to Security Standard SEC525-02, agencies have $0 delegated procurement authority for those procurements which involve third-party (supplier-hosted) cloud services (i.e., Software as a Service). There is a distinct process for obtaining VITA approval to procure these type of solutions: Refer to the Third Party Use Policy at this URL: https://vita.virginia.gov/it-governance/itrm-policies-standards/. Your agency's Information Security Officer (ISO) or Agency Information Technology Resource (AITR) can assist you in understanding this process and in obtaining the required documentation to include in your solicitation or contract. There are specially required Cloud Services terms and conditions that must be included in your solicitation and contract, and a questionnaire that must be included in the solicitation for proposers to complete and submit with their proposals. You may also contact: enterpriseservices@vita.virginia.gov for additional information and assistance.

When does something have to come through Enterprise Cloud Oversight Services (ECOS)?

ECOS is a service specifically created for third party vendors offering Software as a Service (SaaS) applications to agencies.

What is SaaS? Saas is the capability provided to the consumer 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.

- SaaS Characteristics –
    - Network-based access to, and management of, commercially available software
    - Supplier provided services are accessed through an internet connection to a third party hosted facility.
    - Service delivery is typically a one-to-many model (single instance, multi- tenant architecture). The service also generally includes a common architecture for all tenants, usage based pricing, and scalable management.
    - The third party supplies the management of the service which includes functions such as patching, upgrades, platform management, etc.
    - A multi-tenant architecture, all users and applications share a single, common infrastructure and code base that is centrally maintained.
    - The subscriber/user manages access controls for the application.
    - The provider is acting as the data custodian and server administrators for the service.

- What is PaaS? PaaS is the capability provided to the consumer 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.
- PaaS Characteristics –
    - Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to fulfill the application development process
    - Web based user interface creation tools help to create, modify, test and deploy different UI scenarios
    - Multi-tenant architecture where multiple concurrent users utilize the same development application
    - Built in scalability of deployed software including load balancing and failover
    - Integration with web services and databases via common standards
    - Support for development team collaboration – some PaaS solutions include project planning and communication tools
    - Tools to handle billing and subscription management

Other Important Guidance

It is important that the procurement lead understand its agency's and VITA's security policies, standards and guidelines; the technical and functional requirements of the solicitation and/or contract; and, that he or she works in close collaboration with the business owner and security team to ensure inclusion of appropriate terms and conditions to mitigate risks to overall security and data security and privacy for the project.

Ask cloud suppliers as many questions as possible to obtain a thorough understanding of exactly what they are offering (is the service model type SaaS, PaaS, or IaaS); the means by which they are offering it (private, public, hybrid, federal or other); where they will intake, process, store and backup your data at all times (your state, U.S., offshore); and how will they prove to you the maturity and seriousness of their own cloud strategy and operational processes (are they FedRAMP approved, NIST compliant; how will they ensure compliance with your agency's and VITA's security and data privacy requirements, as well as any applicable federal information security and privacy laws and regulations, as mandated by §2.2-2009 of the *Code of Virginia*).