Chapter highlights

Purpose: This chapter provides information about the commonwealth's security and cloud compliance requirements for all agencies when procuring IT. VITA has statutory authority for the security of state government electronic information from unauthorized uses, intrusions or other security threats by developing and implementing policies, standards and guidelines, and providing governance processes and audits to ensure agency compliance.

Key points:

- Adherence to all information security policies, standards and guidelines is required of all state agencies and suppliers providing IT products or services to your agency.
- Also, any procurement of information technology made by the Commonwealth's executive, legislative, and judicial branches and independent agencies shall be made in accordance with federal laws and regulations pertaining to information security and privacy.
- In addition to VITA Security Standard SEC525 for any procurements for third-party (supplier-hosted) cloud services (i.e., Software as a Service), since agencies have $0 delegated authority to procure these types of solutions, there is a distinct process for obtaining VITA approval to procure.
- There are specially required Cloud Services terms and conditions that must be included in any solicitation or contract for cloud services and a questionnaire that must be included in the solicitation for bidders to complete and submit with their proposals.

Table of Contents

28.0 Introduction

Pursuant to § 2.2-2009 of the *Code of Virginia*, the CIO is charged with the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information and that any procurement of information technology

made by the Commonwealth's executive, legislative, and judicial branches and independent agencies is made in accordance with federal laws and regulations pertaining to information security and privacy.

The CIO has given VITA's Commonwealth Security and Risk Management (CSRM) Division the responsibility for developing security-related policies, standards and guidelines (PSGs), implementing them and providing governance processes and audits to ensure agency compliance. VITA's Project Management Division (PMD) and Supply Chain Management Division (SCM) and other VITA divisions participate in various oversight and governance capacities to assist CSRM in fulfilling VITA's statutory security obligations.

28.1 VITA Information Security PSGs required in all IT solicitations and contracts

28.1.1 Application of VITA Security PSGs to all IT solicitations and contracts

Security PSGs are available at: https://www.vita.virginia.gov/it-governance/itrm-policies-standards/. Adherence to the Security PSGs is required. Agency information security officers (ISOs) or agency information technology resources (AITRs) should be familiar with the Security PSGs.

When developing an IT solicitation or contract, the agency procurement lead must ensure the above link is included in the Technical/Functional Requirements section of the document. Use the Minimum Requirements Matrix which you can download from this SCM webpage: https://www.vita.virginia.gov/procurement/policies--procedures/procurement-forms/.

This matrix includes usable mandatory language that points to the Security PSGs link above, as well as mandatory language and links to other VITA PSGs that cover Enterprise Architecture requirements, Data Standards requirements IT Accessibility and 508 Compliance and high-risk contract requirements. Your procurement's project manager, ISO or AITR will know if any formal exceptions will be needed and will obtain any such exception from VITA, should the supplier proposal not be able to comply with any of these requirements.

In addition, if a procurement is a cloud-based procurement (i.e., off-premise hosting), Supplier's failure to successfully answer, negotiate and/or comply with any resulting security exceptions that may arise in order to approve Supplier's cloud application, may result in removal from further consideration.

28.1.2 Enterprise Cloud Oversight Services (COV Ramp) Security Assessments

Cloud oversight security assessments may result in the need for security exceptions to be granted prior to awarding a contract to the supplier. Any security exceptions are confidential and must never be disclosed publicly. The agency is responsible for having any security exceptions approved by VITA Security through Archer. Archer is the VITA tool of record for maintaining an agency's information related to their applications and associated business processes, devices and data set names. Your agency AITR can perform or assist with this process. The Archer User's Guide is available for download here: https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/Archer-User-Manual-2021.pdf.

The Security Assessment may also result in contractual requirements that should be inserted in the Cloud Terms' Supplier Responsibilities section.

You can access the Information Security Policy & Standard Exception Request Form here: Policies, Standards & Guidelines | Virginia IT Agency.

A supplier may request the agency sign a non-disclosure agreement (NDA).In the COV Ramp process, VITA will sign a NDA on behalf of VITA personnel having access to the Assessment details or the Assessment responses and any resulting approval exception(s).

The actual Security Assessments are never to be included in the contract, and extreme care should be taken not to share the Security Assessment with non-stakeholders. Normally, the results of the Security Assessment and its approval and exceptions are not shared with the evaluation Team, as these are not evaluated per se. If a Sourcing Consultant or procurement lead needs to share, it would be wise to reiterate the confidential nature of the Security Assessment responses and any resulting exceptions to stakeholders (in this case, meaning individuals with a need-to- know), or have stakeholders individually sign an NDA, if they have not already signed one as an Evaluation Team member.

28.1.3 Application of policy and procedures to all Cloud Services solicitations and contracts

Information Security Standard (SEC530) provides agency compliance requirements for non-Commonwealth hosted cloud solutions.

For any procurements for third-party (supplier- hosted) cloud services (i.e., Software as a Service, or SaaS), agencies must use the process known as COV Ramp (formerly ECOS). For more information, see https://www.vita.virginia.gov/cov-ramp/

Your agency's ISO or 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 bidders to complete and submit with their proposals. You may also contact: enterpriseservices@vita.virginia.gov

More guidelines and information for COV Rampare available here: https://www.vita.virginia.gov/cov-ramp/

Commonwealth security and cloud requirements and checklists: Procurement Tools | Virginia IT Agency

28.1.4 Cloud Oversight

First under Executive Order Number 19 (2018), Cloud Service Utilization and Readiness, and later under applicable language in the Appropriation Act and VITA's chapter of Title 2.2, VITA developed governance documents in support of a cloud approach that addresses requirements for evaluating new and existing IT for cloud readiness. More information on COV Ramp assessment and oversight is available at https://www.vita.virginia.gov/cov-ramp/ .

28.1.5 Prohibition on the use of certain products and services

Pursuant to Virginia Code § 2.2-5514, public bodies are prohibited from using, whether directly or through work with or on behalf of another public body, any hardware, software, or services that have been prohibited by the U.S. Department of Homeland Security for use on federal systems. More information on prohibited IT is available in SEC528, Prohibited Hardware, Software, and Services Policy.