PURPOSE:	The purpose of this policy and procedures document is to enable the adoption of cloud-based services, where appropriate, across the Commonwealth of Virginia (COV) agencies, as defined by §2.2-2006 of the *Code of Virginia* and legislative, judicial and independent agencies of the Commonwealth and used herein as “agency/ies,” using VITA as an IT service provider. The adoption of cloud computing will include the evaluation of the service provider for adequate IT management as well as cataloging cloud services that have existing contracts with the commonwealth.
BACKGROUND:	The National Institute of Standards and Technology (NIST) defines cloud computing as: “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.” The commonwealth has adopted the NIST definitions as part of the strategic approach to cloud computing. In line with that adoption, cloud services are classified in one of three service models software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). To incorporate services that meet these definitions into VITA’s service portfolio, the cloud evaluation service has been created. This process will evaluate the capabilities of the service requested to provide IT services in a manner consistent with operational and security requirements established by the commonwealth.
SCOPE:	This policy and procedures document applies to all agencies to which VITA provides IT services. It pertains to the request for acquisition of IT services not currently included in the services provided by VITA and that have received all VITA prerequisite governance approvals.

ACRONYMS:

CIO	Chief Information Officer
FTI	Federal Tax Information
HIPAA	Health Insurance Portability and Accountability Act
IT	Information technology
NIST	National Institute of Standards and Technology
IaaS	Infrastructure as a service
PaaS	Platform as a service
PCI DSS	Payment Card Industry Data Security Standard
SaaS	Software as a service
SEC	Security standard
SOW	Statement of work
VITA	Virginia Information Technologies Agency

STATEMENT OF POLICY: **Cloud-based solutions** are considered IT systems and are subject to the same internal audit and security standards as systems and applications hosted on premise.

STATEMENT OF PROCEDURES: **<u>Agency Requirements:</u>**

- **Prior written approval** – Agencies must receive written approval via the VITA enterprise cloud oversight service. prior to procuring, signing or otherwise engaging with a third-party hosted (cloud) service.

- **VITA pre-authorization -** The supplier and requested service(s) must be identified in the VITA enterprise cloud hosting form to ensure the acquisition of cloud-based services, physical or virtual applications, infrastructure network, system components, and any data center facilities have been pre-authorized by VITA.

- **Cloud computing services -** Each request for utilizing IT services not already provided by VITA will be evaluated for adherence to commonwealth requirements, adequate operation of the requested services, and appropriate cloud service procurement terms and conditions.

- **Oversight and governance body** – All use of third-party hosting (cloud computing) services must have an oversight and governance body that is approved by VITA. This governance body will certify that security, privacy and other IT management requirements have been adequately addressed prior to approving the use of external cloud computing services.

- **Approval period -** All third-party hosting (cloud computing) requests are valid for one year unless otherwise specified.

- **Periodic review of hosting services -** All third-party hosting services are subject to periodic review and approval may be revoked at any time. In the case when a supplier or agency is out of compliance with the requirements in this document, any costs incurred by VITA associated with migration or correction of identified compliance issues will be billed to the agency.

- **Enterprise cloud oversight service –** Third-party cloud service requests that have been previously approved via VITA's previous exception process shall be subject to the enterprise cloud oversight service upon expiration of the approved exception request unless otherwise specified by VITA.

- **Policy and procedures periodic review** – This policy and procedures document will be reviewed annually or subsequent to any significant issue arising that has not been previously considered.

Supplier Requirements:

Suppliers are subject to recurring risk assessments at least annually and immediately following any significant issues.

- **Security compliance -** The supplier(s) shall fully comply with all specified security standards in line with the security classifications of the data. Compliance with relevant or mandated third-party standards such as Health Insurance Portability and Accountability Act (HIPAA), Federal Tax Information (FTI) and Payment Card Industry Data Security Standard (PCI DSS) are to be detailed within the supplier's assessment response.

- **Audit requirement -** The supplier shall provide a recently completed audit, preferably a Service Organization Control Type 2 (SOC2). The agency or third-party audit organization is responsible for performing a security audit within 90 days to determine control gaps between the supplied audit and the *Hosted Environment Information Security Standard* (SEC525). If no audit is supplied, a complete security controls audit utilizing SEC525 must be performed. Failure to do so may result in remedies being levied as outlined in the terms and conditions of the contract. The supplier must be obligated to immediately notify the agency and VITA of any security breach via the contractually agreed to procedures. The supplier must prohibit unauthorized access to and use or alteration of the data stored. The method and procedures for this must be outlined in the contractual terms.

- **Chargeback model -** Supplier's service chargeback model must be clearly documented and included as part of the VITA enterprise cloud hosting form. This ensures that all applicable fees and fee structure as they pertain to the service are understood.

- **Control of data** – The supplier shall at all times maintain control of the data and in the event of an enforced default must provide the contracting agency its data in an agreed-upon format and timeframe as specified in the statement of work (SOW). The supplier must provide and maintain non-proprietary interoperability and portability standards defined for information exchange and usage. This requirement is intended to support interoperable components and facilitate migrating applications to and/or from the cloud supplier.

- **Security compliance** – Supplier must comply with all applicable VITA policies and standards as outlined in https://vita.virginia.gov/default.aspx?id=537 to include appropriate state and federal regulations, policies, standards and guidelines (e.g., SEC 501, SEC 525, IRS Publication 1075, NIST Risk Management Framework, etc.) for the protection of commonwealth information and data. This includes ensuring all information system components and services remain within the continental United States. This is intended to enable effectively governance, risk management, assurance, and legal, statutory and regulatory compliance obligations by all impacted business relationships.

Acquisitions:

This policy requires that VITA supply chain management be engaged and involved in any procurement of cloud based services.

- **Contract language approval** – All contract language must be approved by VITA supply chain management.

- **Compliance** – Any contracts for cloud computing services must include language stating the supplier will comply with all commonwealth laws, security requirements, and any applicable federal or industry standards and regulations. Appropriate language must be included in the contract vehicle defining the cloud service provider's responsibilities and the commonwealth's responsibility for maintaining all applicable standards and regulations.

- **Terms and conditions** – VITA supply chain management has cloud service terms and conditions for agency use in acquisition documentation (solicitations and contracts).

- **Term of service agreements** – Terms of service agreements are identified as contract language and as such any term of service agreements must be approved by VITA supply chain management in advance of any agreements being signed. Digital signatures such as clicking "OK" are considered signing a contract and shall not occur prior to contract review.

Continuity Planning:

- **Exit strategies** – Agencies must identify explicit exit plans for each application that is leveraging a non-premise based supplier. Any agency contracting a cloud-based service must engage and coordinate with VITA to ensure that at least two exit strategies are documented for every application or service being used. The first exit plan (required) must be application and supplier specific and will be invoked in the event of a catastrophic failure such as, but not limited to:
  - Significant security breach
  - Supplier bankruptcy
  - Failure to comply with applicable laws and regulations

- **Second exit plan** - The second exit plan may be a single generic plan that is invoked for any application or service that fails to perform adequately and is subject to early termination of the contract. As well, all exit plans must indicate that data uploaded to a cloud service by an agency, its users, citizens of the commonwealth or partners must remain the property of the contracting agency and cannot be used without expressed written permission. It shall also indicate that upon written request of the agency, the supplier shall destroy such confidential information and provide the disclosing agency with written certification of such destruction and cease all further use of the authorized user's confidential information, whether in tangible or intangible form.

Enterprise Integration Requirement:

- **Integration with VITA services** – Every agency contracting with any cloud service provider must integrate with VITA services unless specified otherwise in the approval documentation. This ensures that VITA is aware of the details of any problems with the cloud provider or service and can support the agency in bringing these issues to a close.

ASSOCIATED POLICY/ PROCEDURE: As stated in the *Hosted Environment Information Security Standard* (SEC525), externally provided services/systems and safeguards used in the electronic transmission or storing of commonwealth and/or citizen data must be risk assessed, and security and interoperability must be maintained across all relevant state/national systems.

AUTHORITY REFERENCE: The *Code of Virginia* §2-2.2009 states that "the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information."

OTHER REFERENCE: *IT Information Security Standard* (SEC 501), *Hosted Environment Information Security Standard* (SEC 525), *IRS Publication 1075*, and *NIST Risk Management Framework*

POLICY EXCEPTION REQUESTS: This policy and procedures document requires VITA, agencies and suppliers to work together on reporting and evaluation of emerging risks and issues. If an agency head determines that compliance with this policy would adversely impact the business process of the agency, the agency head may request an exception to the policy or standard by submitting an exception request to VITA. The policy and exception request form is on the ITRM Policies, Standards and Guidelines web page at: http://www.vita.virginia.gov/library/default.aspx?id=537.

Version History		
Version	Date	Change Summary

1	11/30/2016	Original document
1.1	06/23/2016	Revision