Cloud Technology Services Policy
USG Policy 6 (4.10) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to specify guidelines in which the USG must assess, and take steps to mitigate, the risk of unauthorized access, use, disclosure, modification, or destruction of confidential information when using third-party cloud technology services.

This policy applies to all third-party cloud technology service agreements where information will be transmitted, collected, processed, stored, or exchanged with the cloud service provider. Third-party cloud technology services must adhere to USG's Data Classification 6 (2.10) and Confidential Data 6 (2.00) policies.

Other areas covered under this policy include:

- Cloud Services
- Software-as-a-Service (SaaS)
  Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Network-as-a-Service (NaaS)
- Web Hosting
- Application Hosting
- Database Hosting
- Cloud Data Backup
- Offsite Cloud Storage

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as "OIT." This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Cloud Service:* an on-demand service or solution provided by over the Internet (i.e. cloud) which resides and runs on the provider's cloud computing platform and infrastructure. *NOTE: See Appendix B for scope of responsibility for each type of cloud service.*

B. *Mission Critical System*: a system that is vital to the continual successful operation of an organization to the extent that without it would cause significant interruptions to business operations and services.

C. *Control Assessment Report*: a document detailing and assessing an organization's ability and effectiveness to manage risk including the controls in place.

III. Provider Approvals

A. The initiation or introduction of new cloud technology services must be approved by the Director of the Office of Information Technology (OIT) prior to any procurement request, contract signing, and payment to the third-party cloud technology service provider. It is the responsibility of the purchaser or a representative of the department making the purchase, which from this point forward in the policy will also be known as the purchaser, to notify OIT of any new cloud technology services it is attempting to procure. In addition, the purchaser must provide OIT with a technical point of contact who has access and permission to distribute the service provider's applicable security polices, audit records, control assessment reports, and any other documents necessary to insure compliance with USG's OIT security policies and comparable protection requirements for similar premise-based solutions.

B. OIT is responsible for the following tasks regarding new cloud technology service providers:

1. Reviewing a provider's compliance with and the storing of applicable security and audit documentation regarding IT security, privacy, and availability.
2. Assessing the risks associated with the cloud technology service provider.
3. Insuring that the cloud technology service provider follows acceptable control assessment procedures, and if possible, the resulting report is certified by an approved independent audit organization (see Appendix A below for a list of acceptable control assessment reports).
4. Maintaining a master list of approved cloud technology service providers.

IV. Periodic Reviews

A. OIT will conduct periodic reviews of all recent control assessment reports and security documentation to continue to ensure a provider's compliance with any applicable policies and contract deliverables, as well as, reassess the risk of the cloud technology provider's service/solution. This review should be completed at least once per contract cycle, preferably before a renewal of services with the cloud provider.

V. Contract Requirements

A. This section sets general guidelines and requirements for third-party cloud technology service provider contracts. Each contract should include the following:

1. Requirements for recovery of institutional resources such as data, software, hardware, configurations, and licenses at the termination of the contract
2. Service level agreements including provisions for non-compliance
3. Provisions stipulating that the third-party service provider is the owner or authorized user of their software and all of its components, and the third-

party's software and all of its components, to the best of third-party's knowledge, do not violate any patent, trademark, trade secret, copyright or any other right of ownership of any other party

4. Provisions that stipulate that all institutional data remains the property of the institution
5. Provisions that require the consent of the institution prior to sharing institutional data with any third parties
6. Provisions that block the secondary use of institutional data
7. Provisions that manage the retention and destruction requirements related to institutional data
8. Provisions that require any vendor to disclose any subcontractors related to their services
9. Requirements to establish and maintain industry standard technical and organizational measures to protect against:
    - accidental damage to, or destruction, loss, or alteration of the materials;
    - unauthorized access to confidential information
    - unauthorized access to the services and materials;
    - industry known system attacks (e.g., hacker and virus attacks)
10. Requirements for reporting any confirmed or suspected breach of institutional data to the institution
11. Requirements that the institution be given notice of any government or third-party subpoena requests prior to the contractor answering a request
12. The right of the Institution or an appointed audit firm to audit the vendor's security related to the processing, transport or storage of institutional data
13. Requirement that the Service Provider must periodically make available a third-party review that satisfies the professional requirement of being performed by a recognized independent audit organization (refer to Appendix A). In addition, the Service Provider should make available evidence of their business continuity and disaster recovery capabilities to mitigate the impact of a realized risk (if available)
14. Requirement that the Service Provider ensure continuity of services in the event of the company being acquired or a change in management
15. Requirement that the contract does not contain the following provisions:
    - The unilateral right of the Service Provider to limit, suspend, or terminate the service (with or without notice and for any reason)

- A disclaimer of liability for third-party action

16. Requirement that the Service Provider make available audit logs recording privileged user and regular user access activities, authorized and unauthorized access attempts, system exceptions, and information security events (as available).

VI. Restrictions

A. OIT reserves the right to request the immediate termination of use or deny approval of new or renewal of a cloud technology service provider services and solutions at any time provided it can demonstrate non-compliance with any of the following:

1. Contract term deliverables (such as denial of access to the agreed upon security related documentation).
2. Violation of local, state, or Federal law or regulation.
3. Non-compliance with USG, USM, or State IT security policies.
4. Periodic review/assessment of the cloud technology service provider reveals unacceptable risk to USG information or connecting devices and infrastructure.

B. It is strongly recommended that OIT should notify the cloud technology service provider of any violations and with reasonable efforts work with the provider to take any necessary corrective action to bring them back into compliance.

VII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

VIII. Revision History

Date	Description	Revised By
03/28/2018	Initial Policy Creation	Russell Schlosburg
03/15/2019	Replaced 11.1 reference in section 3.3 to Appendix A	Russell Schlosburg

IX. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

B. PCI DSS Virtualization Guidelines v2.0, June 2011. PCI Data Security Standard (PCI DSS)
https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

Appendix A: Acceptable Control Assessment Reports

Report Name	Certifying Organization
AICPA SOC2/Type2	American Institute of CPAs
PCI Security Standards	Payment Card Industry (PCI) Security Standards Council
ISO 27001/2 Certification	International Organization for Standardization (ISO)
FedRAMP	Federal Government (General Services Administration)

NOTE: Any control assessment report not listed above should be submitted to OIT for review of acceptance.

Appendix B: Cloud Service Scope of Responsibility

Cloud customer responsibility	
Cloud service provider responsibility	

	Type of Cloud Service		
Area of Responsibility	IAAS	PAAS	SAAS
Data			
Software, user applications			
Operating systems, databases			
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)			
Computer and network hardware (processor, memory, storage, cabling, etc.)			
Data center (physical facility)			

Source: PCI DSS Virtualization guidelines, 2011