UMES-Cloud Services Policy

University of Maryland Eastern Shore

Cloud Services Security Policy

Date: November 14, 2018

1. PURPOSE

Organizations are increasingly moving infrastructure and operations to hosted providers in order to provide data and tools to employees efficiently and cost-effectively. The security posture of **Cloud Service Providers (CSP)** must be assessed in order to determine compliance with University of Maryland Eastern Shore (UMES) security requirements before University of Maryland Eastern Shore Information Technology (UMES IT) department managed infrastructure can be hosted outside of the University of Maryland Eastern Shore environment.

UMES IT is responsible for, and committed to, managing the confidentiality, integrity, and availability of UMES networks, systems, and applications within the scope of its authority. This includes ensure wherever possible that cloud environments hosting University of Maryland Eastern Shore infrastructure meet specified security controls and do not endanger the security posture of the University.

2. SCOPE

This policy is applicable to all UMES IT Systems that are hosted in cloud infrastructure. UMES IT will be responsible for enforcing the security of cloud environments wherever possible in accordance with the requirements in this policy. **Any UMES department that is considering the purchase of a cloud based system should confer with UMES IT before purchasing.**

3. BASE POLICY AND COMPLIANCE REFERENCES

UMES IT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as UMES's authoritative adaptation of these policies with specific amendments to

meet the business and operational needs of the University.

Policy References

State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy- List.aspx

USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

4. POLICY

When multiple organizations use a single CSP, organizations can benefit from an economy of scale. However, using a CSP centralizes management of information and applications as data and processing are shifted out of the direct control of formerly distinct IT and security groups. When utilizing a shared CSP, security teams must institute a set of (CSP and operational) controls as directed in this policy to govern and mitigate risks, helping to ensure the safety of University of Maryland Eastern Shore, operations, and IT resources.

Cloud computing solutions used by University of Maryland Eastern Shore should have the configuration, deployment, and management structures than can meet the University's security, privacy, and other requirements wherever possible in order to access or store confidential data.

4.1 Preliminary Requirements

All cloud providers utilized by UMES IT systems that will access Personally Identifiable Information (PII) data as defined in the *UMES Public & Confidential Data Classification Policy* must meet the minimum requirements outlined below.

# Name	Requirement
A Compliance with UMES Security Standards	Cloud providers must be able to comply with requirements as established within the relevant UMES IT Security Policies, including this document.

B UMES IT Authorization	A security review of the cloud service must be conducted by UMES IT prior to the procurement of the service.
C Classification of Data	Agencies must anticipate and mitigate risks where possible of cloud-hosted data and resources in accordance with the *UMES Asset Management Policy*, and *UMES Security Assessment Policy*.

4.2 Vendor Assessment

UMES IT will assess a CSP that will be accessing UMES IT managed PII data to ensure the CSP can operate with the requirements outlined below.

# Name	Requirement
A Assess Competency of Provider	UMES IT must exercise due care and due diligence and conduct a thorough analysis of the provider's capabilities and security measures. This can be done through means such as: Detailed questionnaire given to the CSP Research into the company External vendor-assessment reports or audit results Previous client testimonials
B Establish Contractual Obligations	CSPs may have standard contractual language, however it is important that wherever possible, UMES IT should negotiate with CSPs to insert UMES security controls into contract language if not already covered. Contracts should be re-evaluated upon any significant change to the CSP as a third-party entity (e.g., bought by another company, bankruptcy)
C Continuous Assessment	Where possible, UMES IT should negotiate with CSPs to allow for ongoing evaluation by the UMES IT to ensure that security measures are properly implemented and enforced. Any violation of security measures affecting the security of UMES information or resources that is discovered by UMES IT must be communicated with the CSP as soon as possible after discovery so the CSP can address the concern.
D Regulatory Compliance	CSPs should, as part of their UMES IT assessment, be able to demonstrate compliance with applicable regulatory requirements such as: PCI DSS, HIPAA, **CSA**, **SSAE16** (SOC1-financial, SOC2-IT controls, SOC3-attestation), or **ISO**.

4.3 Privacy and Security Controls for Cloud Hosting

UMES IT will assess a potential cloud service provider that will be accessing UMES IT managed PII data to ensure the CSP can operate with any applicable capabilities and functionalities outlined below. These may be included in the questionnaire or other assessment methodologies of the potential CSP as deemed relevant by UMES IT in their evaluation.

# Name	Requirement
A Electronic Discovery	Ensure that cloud provider's electronic discovery capabilities, processes, and policies do not compromise the privacy and security of UMES PII data hosted by the CSP.
B Continuous Monitoring	Where possible, ensure hosted systems or services will allow UMES IT to monitor the services for uptime, availability and security functionality.
C Architecture	UMES IT should understand applicable underlying technologies that the cloud providers use to host services and how that integrates with current UMES on premise infrastructure if such integration exists.
D Identity and Access Management	Ensure relevant safeguards are in place to secure authentication, authorization, and other identity and access-management functions in accordance with the requirements outlined in the *UMES Account Management Policy* and *UMES Data Security Policy.*

E Software and Data Isolation	CSPs should certify that in multi-tenant offerings the structure or architecture of their systems are capable of isolating hosted data and operations from other tenants where possible.
F Availability	Establish an SLA with the CSP for notification of service disruption as well as resumption of critical operations within an agreed upon time.
G Incident Response	Ensure that the cloud provider informs UMES IT within a reasonable time after a breach has been discovered that directly impacts the agency resources or data.

5. EXEMPTIONS

If an exemption from this policy is required, an UMES IT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

6. DEFINITIONS

Term	Definition
Cloud Service Provider (CSP)	A company that offers some component of cloud computing — typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) — to other businesses or individuals.
International Organization for Standardization (ISO)	An international standard-setting body composed of representatives from various national standards organizations which promotes proprietary, industrial, and commercial standards.
Standards for Attestation Engagements No. 16 (SSAE16)	Auditing standard for service organizations, often used to report compliance with Sarbanes Oxley Act.
Operating System (OS)	A system software that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer.

7. ENFORCEMENT

UMES IT is responsible for managing security assessments for the University according to established requirements authorized in the UMES IT Security Program Policy. Any systems under the policy authority of UMES IT with requirements

that deviate from the UMES IT Security Program policies are required to submit a Policy Exemption Form to UMES IT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.

Cabinet approval pending. 12/13/18