Carnegie Mellon University

Updates to Public Cloud Service Enterprise Policy

Pragya Mittal

October 1st, 2025

Heinz College of Information
Systems and Management
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213

Advised by:

Matthew Butkovic

John Haller

1 Purpose and Scope

This paper assesses Carnegie Mellon University's existing cloud service enterprise policies and provides requirements and recommendations in light of the ongoing negotiations to switch cloud service providers. It also aims to establish a standardized approach for selecting, managing, updating, and enforcing cloud security policies in case of migration to a different platform in the future. The updated policy will apply to all students, faculty, non-faculty staff, and other individuals affiliated with Carnegie Mellon University (CMU) using cloud services for university-related activities.

2 Stakeholders

The policy creation for the new cloud service provider would be championed by the Office of the Chief Information Officer (CIO), since the existing Information Security Policy of the university has been drafted under them. Other stakeholders of this policy are the external cloud service providers and third-party vendors.

The success of this policy hinges on the endorsement of key top-level management executives within the university, such as:

- President (currently Farnam Jahanian),
- Vice President for Information Technology and Chief Information Officer (currently Stan Waddell),
- Assistant Vice President and Chief Information Security Officer (currently, Mary-Ann Blair),
- Vice President for Research (currently Theresa S. Mayer), and
- Vice President for Finance and Chief Financial Officer (currently Angela Blanton).

We would also need alignment from external stakeholder representatives of the cloud service provider the university selects, such as:

- Cloud Service Provider Account Executive
- Cloud Service Technical Architects
- Third-Party Software Vendors
- Compliance and Regulatory Officers
- Service Support Team Representative

3 Analysis of Current Cloud Policies

CMU currently has two publicly available policies regarding cloud usage. The first is the Public Cloud Services page (CMU, 2025), which outlines relationships with approved providers such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure, addresses billing and provisioning, and briefly references data classifications (Public, Private, Restricted). The other is the Guidelines for Cloud Computing page (CMU, 2021), which talks about the relationship the university has with two cloud service providers – namely, Dropbox and Google Cloud.

Neither of these artifacts provides a comprehensive policy on cloud usage within the university. They read more as guidelines than as actionable, enforceable enterprise-level policies. There is no mention of third-party or cloud vendor risk, no contractual oversight, or policies for continuous monitoring. There is also no explicitly defined shared responsibility boundary or formal service-level agreement (SLA) with measurable resilience metrics. The existing materials also do not address technical baselines or compliance requirements. There is also no mention of disaster recovery or business continuity in the event of a disaster. An ideal policy should also have documentation on an exit strategy if required.

The following sections discuss the requirements for writing a robust public cloud service enterprise policy and list the recommended sections the policy should include.

4 Requirements for Cloud Vendor

This section outlines the different functional, non-functional, and security requirements the selected cloud vendor must satisfy to be considered appropriate to be adopted university-wide.

4.1 Functional Requirements

CMU needs to define what cloud services need to do to meet the university's operational needs. This section would clearly outline the technical requirements, like compute size, number of VMs, GPU/CPU requirements, autoscaling policies, etc. CMU will also need to conduct an assessment of its storage needs and the type of storage they require (high-performance storage, backups and redundancy, archival options). Other considerations would address questions like the extent of collaboration tools (emails, collaboration suites, etc.).

4.2 Non-Functional Requirements

This section of the policy should explicitly state expectations about the quality of service the cloud service provider offers beyond basic technical functionality. For instance, service-level expectations, like uptime, latency, mean time to recovery (MTTR), mean time between failures (MTBF), and disaster recovery capabilities need to be stated. Cost management is another key factor to consider. There needs to be transparent pricing and options for cost

optimization. Finally, support and service capabilities are essential, including 24/7 technical support, access to dedicated account managers, and training resources to help university staff and faculty use the cloud platform.

4.3 Security and Compliance Requirements

The selected cloud service provider must strictly adhere to all relevant security and compliance standards and laws applicable to the cloud service providers and the university in the state of Pennsylvania and the United States. These include, but are not limited to:

- ISO/IEC 27001: Information Security Management Systems (ISO, 2013)
- ISO/IEC 43757: IT Security Techniques for Cloud Services (ISO, 2013)
- ISO/IEC 76559: IT Security Techniques for Personally Identifiable Information (PII) in Public Clouds (ISO, 2014)
- PCI DSS: Payment Card Industry Data Security Standard for secure payment processing (PCI Security Standards Council, 2022)
- NIST Cloud Security Guidance for Small Businesses (NIST, 2021)
- NIST SP 800-210: General Access Control Guidance for Cloud Systems (NIST, 2020)
- CIS Benchmarks for Cloud Security (Center for Internet Security, 2022)
- CIS Critical Security Controls (Cloud Companion Guide) (Center for Internet Security, 2022)
- Cloud Security Alliance STAR Program: Security, Trust, and Assurance Registry (Cloud Security Alliance, 2021)
- FedRAMP Partners: Compliance for federal data security standards (FedRAMP, 2022)

In addition to these, the cloud service provider must also be compliant with data privacy laws such as FERPA, HIPAA, and FISMA. They should also implement strong encryption with a key size of over 128 bits. The cloud service provider should also provide multi-factor authentication, role-based access, and identity & access management.

For logging and monitoring, the university and cloud service providers need to come to a mutual agreement about their responsibilities within the cloud environment. Typically, it is recommended that the cloud service provider maintain logs of the underlying infrastructure, such as the servers, network, storage, and virtualization layers, while the university would be responsible for the application and database level logs. The details can be codified into the updated policy upon granular agreement.

The cloud service provider should also provide a System and Organization Controls (SOC) Reporting, Type 2 report to the university at agreed-upon regular intervals (Butkovik, 2025).

5 Recommendations

Below are the sections recommended to be a part of the updated cloud service enterprise policy

5.1 Purpose, Scope, and Applicability

The policy should begin with a clear **purpose, scope, and applicability** section. The scope should encompass all cloud service models and deployments (IaaS, PaaS, SaaS) across all academic, administrative, and research domains, including sponsored research environments. To close governance gaps noted in the current guidelines (CMU, 2021), there needs to be an explicit outline of applicability to faculty, staff, students, and contractors.

5.2 Roles & Responsibilities

The policy should formalize the **roles and responsibilities** of all parties involved. It should mention the individuals overseeing the policy, set the frequency of policy reviews, and who would have final authority over it, and the triggers of policy reviews (like major events). It should mention the data owner, steward, and custodian. It should state who has the power to make decisions, select vendors, approve contracts, etc. There should also be a mention of the individuals representing the cloud vendors and their responsibilities. Finally, the responsibilities section to have a catch-all section which enumerates the other parties involved (like computing services, faculty, staff, researchers, students, etc.), and outline their responsibilities.

5.3 Data Classification and Handling

The current Public Cloud Services page (CMU, 2025), briefly mentions the sensitivity levels of data. This should be updated to include more granular categories like regulated data, personally identifiable data, health data, controlled data, etc. It should detail rules around storing, processing, and transmitting data like acceptable encryption levels and key management. It should also discuss data retention policies addressing what kind of data the cloud vendor can store, for how long, and when to delete it.

5.4 Shared Responsibilities and Controls

This section should include what the cloud service provider is responsible for and what the university is responsible for. Shared responsibility is essential to avoid gaps. Many cloud breaches occur due to misconfigurations or mis-assumed responsibilities. Standards like FedRAMP's customer responsibility matrix formalize this. The policy should also add in guidance for departments that spin up their own cloud usage to follow the matrix.

5.5 Security Controls

Controls must cover all security aspects of the cloud. These can range from identity and access management (MFA, least privilege), network segmentation, vulnerability management, to automated configuration monitoring. Logs should be retained in a tamper-resistant form and integrated into CMU's centralized monitoring framework. CSPs must support forensic access and event correlation. The policy should call for the integration of logs generated by the cloud platform with institutional SIEM tools. NIST SP 800-61r2 (Computer Security Incident Handling Guide) and NIST SP 800-137 (Information Security Continuous Monitoring) provide templates for defining monitoring and response expectations (NIST, 2012; 2011). Regular penetration testing, code review, and red team assessments must be institutionalized, reflecting the emphasis of CERT-RMM on maturity and repeatability (Caralli et al., 2016).

5.6 Compliance, Legal and Regulatory Obligations

The policy should dictate that cloud contracts must support compliance with FERPA, HIPAA, GDPR, and export-control regulations (ITAR/EAR). It should require that the providers demonstrate ISO/IEC 27001 and SOC 2 certifications and agree to support compliance audits. Concrete data breach notification timelines (like within 72 hours) and cooperation during investigations must be specified in the policy. The ISACA IT Auditing Guide G4, cited by Butkovic (2024) stresses that outsourcing agreements must grant customers audit and control rights equivalent to internal operations, which should also be reflected in the policy.

5.7 Business Continuity and Disaster Recovery

Building on Presidential Policy Directive 21 and CERT-RMM guidance, resilience requires both protection (preventing disruptions) and sustainment (continuing operations despite disruptions) (Butkovic, 2024). SLAs must specify Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and vendors must provide evidence of tested disaster recovery plans. The policy should require periodic failover testing and integration with campus incident management processes.

5.8 Interoperability, Portability, and Exit Strategy

The policy must require open standards, data export tools, and documentation that support migration between providers. Lewis (2013) emphasized at SEI that "standards are essential for cloud computing interoperability" and that vendor lock-in is a critical organizational risk. An exit plan must define timelines and responsibilities for data retrieval, verification of deletion, and transition to alternative platforms.

6 Conclusion

Carnegie Mellon University prides itself as a steward and pioneer of technological advancements and the responsible handling of the same. This can be exemplified by artifacts like the Tradecraft Report and the CERT Resilience Management Model (Caralli et al., 2016). In cadence with this, the university must have a cloud adoption policy to avoid conflating cloud security risks with enterprise risk.

CMU's existing guidance provides a foundation, but not the mature, integrated framework required for operational resilience. A new Public Cloud Service Enterprise Policy should explicitly define governance, risk management, contractual, and technical requirements that institutionalize resilience and accountability across the entire supply chain.

This document should act as a starting point for drafting a robust and comprehensive cloud service enterprise policy. It provides Carnegie Mellon University with a strategic blueprint for governing cloud usage, ensuring operational resilience, and establishing a clear plan of action in the event of cloud service misuse or compromise.

References

Butkovic, M. (2024). Operational Resilience and Supply Chain Risk Management Lecture Slides. CMU SEI.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2016). CERT Resilience Management Model (CERT-RMM), Version 1.2. Software Engineering Institute, Carnegie Mellon University.

Center for Internet Security. (2022). CIS benchmarks for cloud security. (https://www.cisecurity.org/cis-benchmarks)

Center for Internet Security. (2022). CIS critical security controls: Cloud companion guide. (https://www.cisecurity.org/controls)

Cloud Security Alliance. (2021). CSA STAR program: Security, trust, and assurance registry. (https://cloudsecurityalliance.org/star/)

CMU. (2021). Guidelines for Cloud Computing. Carnegie Mellon University Information Security Office. (https://www.cmu.edu/iso/governance/guidelines/cloud-computing)

CMU. (2025). Public Cloud Services. Computing Services. (https://www.cmu.edu/computing/services/infrastructure/server/public-cloud/index.html)

Ettinger, J., et. al. (2019, May 21). Cyber Intelligence Tradecraft Report: The state of cyber intelligence practices in the United States (Study report and implementation guides). Software Engineering Institute, Carnegie Mellon University.

FedRAMP. (2022). FedRAMP partners: Compliance for federal data security standards. (https://www.fedramp.gov)

International Organization for Standardization. (2013). ISO/IEC 27001: Information security management systems. (https://www.iso.org/standard/54534.html)

International Organization for Standardization. (2013). ISO/IEC 43757: IT security techniques for cloud services. (https://www.iso.org/standard/54536.html)

International Organization for Standardization. (2014). ISO/IEC 76559: IT security techniques for personally identifiable information (PII) in public clouds. (https://www.iso.org/standard/62083.html)

Lewis, G. A. (2013). The Role of Standards in Cloud-Computing Interoperability. Software Engineering Institute, Carnegie Mellon University.

National Institute of Standards and Technology (NIST). (2011). SP 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations. Gaithersburg, MD.

National Institute of Standards and Technology (NIST). (2012). SP 800-61r2: Computer Security Incident Handling Guide. Gaithersburg, MD.

National Institute of Standards and Technology (NIST). (2020). NIST SP 800-210: General access control guidance for cloud systems.
(https://csrc.nist.gov/publications/detail/sp/800-210/final)

National Institute of Standards and Technology (NIST). (2021). NIST Cloud Security Guide for Small Businesses.
(https://csrc.nist.gov/publications/detail/nistir/8286/final)

PCI Security Standards Council. (2022). Payment card industry data security standard (PCI DSS). (https://www.pcisecuritystandards.org)