University of CINCINNATI	*Policy Title:* **Infrastructure, Platform and Software as a Service**	*Policy Number:* **9.1.5**
Category: Information Technology **Policy applicable for:** Faculty, Staff, Affiliates	**Effective Date:** Draft as of 05/25/2017 **Prior Effective Date:** N/A	**Policy Owner:** VP & CIO, UC Information Technologies **Responsible Office(s):** IT@UC Office of Information Security

DRAFT

Background

Infrastructure as a Service, Platform as a Service and Software as a Service offer a number of advantages including low cost, high performance, and quick delivery of services. However, security controls are required to protect university information technology resources.

Infrastructure as a Service (IaaS) refers to solutions that provide services such as storage, virtual server hosting, networking, or other infrastructure components via the internet. IaaS offers many advantages, including scalability based on resource demands.

Platform as a Service (PaaS) allows customers to develop, run, and manage applications without building and maintaining infrastructure. PaaS provides methods to interact with services like databases and file storage, without having to deal with low level requirements.

Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed to or on behalf of the university and is hosted by the vendor, typically the university accesses the application via a web browser.

Policy

This policy addresses the use of IaaS, PaaS, and SaaS for university enterprise purposes where the service essentially becomes an extension of the university network.

Faculty, Staff, and Affiliates are not permitted to enter into IaaS or PaaS service

contracts for the storage, manipulation, or exchange of university data. University departments who need IaaS or PaaS services must use the IaaS and PaaS vendors that have been vetted and contracted by IT@UC.

Purchases of SaaS services require a Security Review prior to implementation. Failure to adequately plan for the security review will result in delay or termination of the project.

Use of IaaS, PaaS and SaaS for the purpose of teaching and instruction is permitted. The academic use must not use Export Controlled, Restricted, or Controlled data, as classified by the Data Governance & Classification Policy.

The following safeguards are required:

- The use of IaaS, PaaS, and SaaS services must comply with the university's existing computing policies. These policies include but are not limited to:
    - Data Governance & Classification Policy
    - Acceptable Use of University Information Technology Resources Policy
      Other information Technology Policies
- The use of IaaS, PaaS, and SaaS services must comply with all laws and regulations governing the variety of data types used by the university.
- Export Controlled data may not be stored in Cloud based file storage unless specifically approved by the Export Controls Office.
- Personal cloud service accounts may not be used for the storage, manipulation, or exchange of university-related communications or university-owned data.
- Data stored in the cloud and data in transit to and from the cloud, must be encrypted.
- Privileged access users accessing the management console or other privileged access accounts in the cloud, must use multi-factor authentication.

Vendors for IaaS or PaaS services are vetted and contracted on an enterprise contract for the university. The vendor must accept the terms as stated in the Data Security Rider. The terms of use for SaaS vendors must be closely scrutinized to ensure adequate protection of the confidentiality, integrity, and availability of university data.

IaaS, PaaS, and SaaS services must not be engaged without developing an exit strategy for disengaging from the vendor or service, and integrating the service into business continuity and disaster recovery plans. The university must determine how data would be recovered from the vendor and/or transferred to a different vendor. The university must also work with the vendor to establish procedures on data sanitization from the vendor's services. Each college or department must follow an appropriate records retention schedule that dictates when different types of

DRAFT

information may be discarded or destroyed as defined by General Records Retention Schedule.

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

Related Links

Acceptable Use of University Information Technology Resources Policy
Data Governance & Classification Policy
Data Security Rider
Purchasing Policy
Security Review

Appendix

IaaS PaaS and SaaS Definitions

Revision History

Draft: 04/24/2017

DRAFT

Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) all aim to shift the local hosting and management of IT Services from on-site to the cloud. The combination of these services is known as the Cloud Services Stack, and each service fulfills its own role in replacing an on-site solution with a cloud based one.

Infrastructure as a Service (IaaS) refers to the fundamental building blocks of Cloud Services. IaaS offers an alternative to locally owned and hosted servers, and users of an IaaS service can build a "virtual datacenter" that has access to many of the same resources as a traditional datacenter without the large upfront investment and space constraints. IaaS is the "lowest level" of the Cloud Services stack, and acts as the "foundation" for all the other segments of cloud services. Examples of IaaS would include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Platform as a Service (PaaS) is one level above IaaS in the Cloud Services stack. A PaaS solution would provide the environment for which the service or program will run, such as the operating system and all necessary software. PaaS is built on top of virtualization technology, which enables efficient hosting and on-demand scaling. IaaS is strictly concerned with hardware and storage devices and PaaS consists of virtual machines that are already loaded with all necessary operating systems and supporting software. Some examples of PaaS include Cloud Foundry, Google App Engine, and Microsoft Azure.

Software as a Service (SaaS) is the highest level of the Cloud Services stack and includes pre-packaged software that the University licenses directly from a vendor. Typically, the university accesses the application via a web browser. SaaS is the highest level of the Cloud Services stack, and moves the task of managing and deploying software to a third-party service. Examples of SaaS include Salesforce, Google Docs, and cloud storage portals like Box or Dropbox. Using SaaS means the customer is not responsible for hosting, updating, or troubleshooting the software, as it is supplied, ready-for-use, by the vendor.

DRAFT