University of CINCINNATI	*Policy Title:* **Cloud Computing**	*Policy Number:* **9.1.5**
Category: Information Technology **Policy applicable for:** Faculty, Staff, Affiliates	**Effective Date:** 09/03/2021 **Prior Effective Date:** 09/25/2019	**Policy Owner:** VP & CIO, UC Information Technologies **Responsible Office(s):** IT@UC Office of Information Security

Background

The purpose of this policy is to ensure that University data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing is a computing model that allows for easy, on-demand computing resources (networks, servers, storage, applications and services) that can be quickly provisioned and de-provisioned with minimal interaction and is accessible to users via the internet. Cloud computing can be defined as the utilization of servers or information technology hosting of any type that is not controlled by the University.

Policy

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.

Use of cloud computing for the purpose of teaching and instruction is permitted. The academic use must not use Controlled Unclassified Information, Restricted, or Controlled data, as classified by the Data Governance & Classification Policy.

Due to security concerns with cloud computing, purchases require a Security Review prior to implementation. Purchasers need to allow time for the security review to avoid any delays.

All cloud computing service must be contracted through centralized university processes. Cloud vendors are vetted and contracted on an enterprise contract for the university. The Data Security Rider must be added to the contract. The terms of

use for SaaS vendors must be closely scrutinized to ensure adequate protection of the confidentiality, integrity, and availability of university data.

The following safeguards are required:

- The use of cloud computing 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 cloud computing services must comply with all laws and regulations governing the variety of data types used by the university.
- Controlled Unclassified Information must be stored and accessed in a manner that complies with NIST 800-171 controls. Additional information about NIST 800-171 can be found in the NIST 800-171 Compliance Guideline.
- Export Controlled data may not be stored in Cloud based file storage unless specifically approved by the Export Controls Office.
- Non-university 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 when technically feasible.
- Privileged access users accessing the management console or other privileged access accounts in the cloud, must use multi-factor authentication.

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

The University has many federal laws that it must follow, these include the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA). A relationship with a cloud-computing vendor may also be impacted by private industry regulations. For example, departments at the University that accept credit cards also must follow the Payment Card Industry (PCI) Data Security Standard (DSS) issued by the major credit card companies. Finally, cloud-computing services that use, store, or process University data must also follow applicable University policies

including but not limited to the Data Governance & Classification Policy.

Definitions

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.

Function as a Service (FaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage application functionalities without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

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