University of
Central
Florida

Office of the President

SUBJECT: Procurement and Use of Cloud Computing and Data Storage Services	**Effective Date:** 6/3/2016	**Policy Number:** 4-014
	Supersedes:	**Page** **Of** 1 4
	Responsible Authority: Vice President and Chief Information Officer	

APPLICABILITY/ACCOUNTABILITY

This policy applies to all individuals working for or on behalf of the University of Central Florida who maintain or use university data. This includes all full-time and part-time employees, adjuncts and others on temporary or time-limited appointments, all volunteers and courtesy appointees, student workers, and all persons paid by or through the university such as contractors, consultants, or employees of Direct Support Organizations.

BACKGROUND

Cloud computing is an application or infrastructure resource that users access via the internet. Although they may be convenient, cloud computing services can bring risks such as data disclosure, data loss, or data compromise. The acquisition and use of a cloud-based service requires a detailed review by the Information Security Office and the Office of the General Counsel. This policy establishes the requirements and procedures necessary to ensure associated risks are managed appropriately.

POLICY STATEMENT

If a department, division, school, or college needs to acquire a cloud-based service that will store, process, or share, university data they must work with the Information Security Office and the Office of the General Counsel to properly evaluate and manage the associated risks and agreement language. Using cloud computing services to handle university data does not absolve a unit from the responsibility of ensuring that the data are properly and securely managed.

UCF is obligated by law and other data security requirements from the Federal Government and certain contractual obligations to protect restricted university data. These data types are described in Data Classification and Protection policy (4-008.1), where they are referred to as “Highly Restricted or Restricted” data. Cloud-computing services must not be used with either of these sensitive data types, unless they are reviewed and approved by the Information Security Office, and the university has entered into a binding agreement with a cloud service provider that is approved by the Office of the General Counsel. Further, the cloud service provider must be able to meet university IT and security standards and may need to be integrated with the university’s identity and access management systems or Enterprise Resource Planning (ERP) systems.

Any violation of this policy and procedures may result in immediate loss of network and computer access privileges, seizure of equipment, loss of research laboratory access, and removal of inappropriate information posted on university-owned computers or university-supported Internet sites.

CONTRACTS OR BUSINESS AGREEMENTS

Any contract or business agreement with a cloud service provider must incorporate the following:

a. the requirement to comply with applicable federal, state, and local laws;
b. the confidentiality, integrity, and availability of the data is maintained;
c. the restricted university data elements to which the cloud-based service provider will have access;
d. the technical means by which restricted university data will be protected;
e. the exact geographic location(s) where university data will be stored;
f. an acceptable method for the return, destruction, or disposal of university restricted data in the cloud based service provider’s possession at the end of the contract;
g. a requirement that the cloud-based service provider must use university restricted data only for the purposes specified in the business agreement;
h. university restricted data acquired in the course of the contract cannot be used for a third-party provider’s own purposes or divulged to others without prior university consent;
i. UCF maintains ownership of data throughout the contract duration;
j. cloud service provider produces an acceptable industry recognized audit report, such as Service Organization Control(SOC)3;
k. cloud service provider shows evidence of current liability or cybersecurity insurance.

Cloud service providers may require users to consent to an end user license agreement (EULA), frequently via a "click-through" agreement, which is a legal contract. Employees covered by this policy are not authorized to enter into legal contracts on behalf of UCF and may not consent to click-through agreements for the purposes of university business. Such agreements should be sent to General Counsel for review.

UCF negotiates agreements with certain cloud service providers. Examples include: Canvas, Knights email, Qualtrics, etc. The terms of these services are clearly defined and represent vetted and authorized cloud services.

DEFINITIONS

Cloud Computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Examples include Microsoft Azure, Amazon Elastic Compute Cloud (EC2), and Google Compute Cloud.

Cloud Data Storage. On-demand network access to a pool of vendor-provided data storage facilities. Examples include Amazon Simple Storage Service, Dropbox, iDrive, Box, and Microsoft OneDrive for Business.

Cloud Services Delivery Models. Cloud computing and data storage services are typically provided in one of three delivery models:

1. Software as a Service (SaaS). Use of the provider's software applications running on the provider's cloud computing infrastructure.
2. Platform as a Service (PaaS). The ability to deploy consumer created or acquired software applications running on the provider's cloud computing infrastructure.
3. Infrastructure as a Service (IaaS). Computing, storage, networking and other infrastructure on which the consumer can run arbitrary software applications, with extensive control over configuration parameters.

Computing resource. Personal computers, laptops, and portable computing and communication devices, servers, mainframes, data storage systems, and similar equipment capable of processing, accessing, displaying, or communicating electronic information.

Electronic information resource. Data or information in electronic format and the computing and telecommunications resources through which such resources are accessed or used.

PROCEDURES

The following steps should be followed when procuring cloud-based services:

a. college or departmental IT units and functional business units must be notified prior to any acquisition involving cloud-based services for review and feedback;
b. units must complete the "UCF Department Questions" section explaining the business justification for using the cloud-based service and coordinate completion of the "Vendor Questions" section of the Third-Party Data Security Assurance Questionnaire for submission to the Information Security Office;
c. the Information Security Office will review and provide a risk assessment to the appropriate data and business owners;
d. the appropriate data and business owners will provide a signed acknowledgement of the risk assessment;
e. the questionnaire and signed risk assessment must be attached to the appropriate purchasing document.

At the discretion of the university, cloud service providers may need to recertify by periodically updating the Third-Party Data Security Assurance Questionnaire.

RELATED DOCUMENTS

Policy 2.100.4 - *Florida Public Records Act—Scope and Compliance Policy*
Policy 2-102.2 - *Contract Review Policy*
Policy 2-103 - *Use of Copyrighted Material Policy*
Policy 3-206.4 - *Credit Card Merchant Policy*
Policy 4-007.1 - *Security of Mobile Computing, Data Storage, and Communication Devices Policy*
Policy 4-008.1 - *Data Classification and Protection*
Policy 4-002.1 - *Use of Information Technologies & Resources Policy*

"The NIST Definition of Cloud Computing," *National Institute of Standards and Technology Publication 800-145, September 2011.*

Records retention schedule - *http://dlis.dos.state.fl.us/barm/genschedules/gs05.doc*

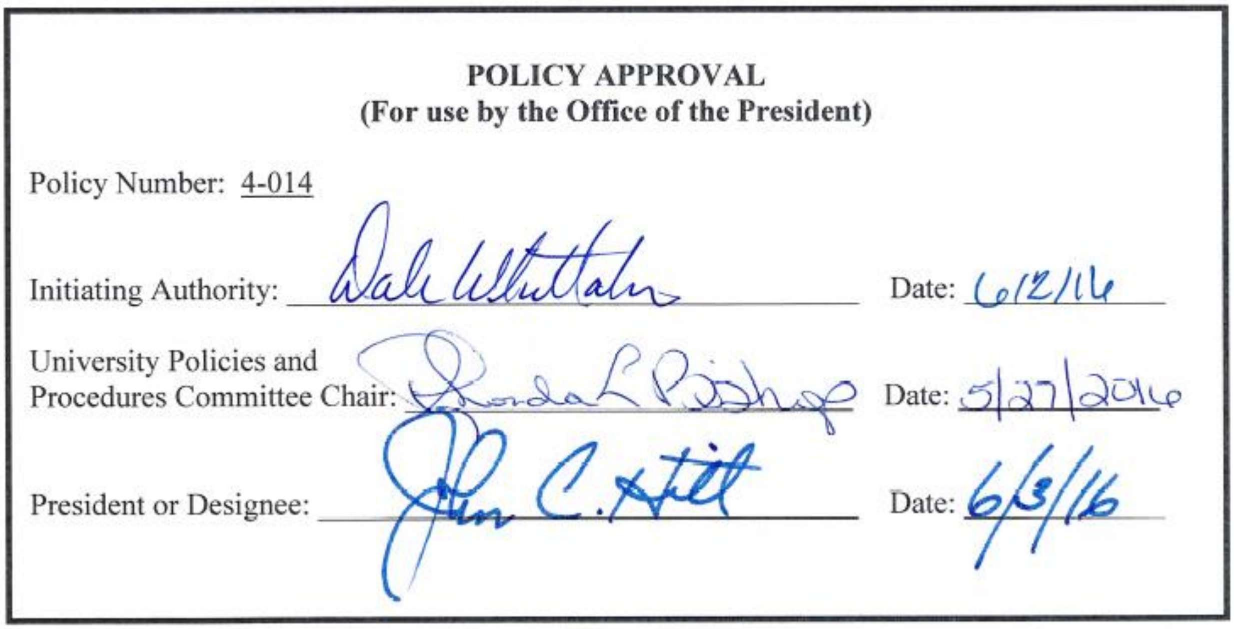
Third-Party Data Security Assurance Questionnaire:
http://www.cst.ucf.edu/wp-content/uploads/Third-Party-Data-Security-Assurance-Questionnaire.xlsx

Secure Handling of University Data:
http://www.cst.ucf.edu/wp-content/uploads/Secure-Handling-of-UCF-Data.pdf

CONTACTS

Computer Services and Telecommunications, Information Security Officer, 407-823-3863

INITIATING AUTHORITY Provost and Executive Vice President for Academic Affairs



POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-014

Initiating Authority: Dale Whittaker Date: 6/2/16

University Policies and
Procedures Committee Chair: Rhonda L Bishop Date: 5/27/2016

President or Designee: John C. Hitt Date: 6/3/16