

SUBJECT:	Effective Date:	Policy Nun	Policy Number:	
CLOUD SERVICE PROVIDERS	10-29-18	12	12.9	
	Supersedes:	Page	Of	
	New	1	3	
	Responsible Authority:			
		Associate Provost and Chief Information Officer, Office of Information Technology		

### APPLICABILITY/ACCOUNTABILITY:

This policy applies to all University colleges, departments, units or organizations seeking to utilize a cloud service provider that processes and/or stores University data, including, but not limited to, student records, personally identifiable information, and personal health information. The purpose of this policy is to provide details on the vetting process of any cloud service provider.

## **POLICY STATEMENT:**

A cloud service provider is a provider that provides alternatives to on-campus resources at an off-site location. This includes software hosted off-site, storage hosted off-site, and other services hosted off-site. Some software products or services that are located on an FAU campus and used locally on an FAU campus may provide some functionality from the cloud, but that functionality does not make the product or service a cloud service provider.

Cloud service providers are a popular alternative to storing or processing data on-site at FAU. FAU encourages colleges and departments to consider cloud service offerings when evaluating new information processing or storage requirements. However, due to the loss of direct control of University data, FAU is required to take measures to ensure the security of information stored at cloud service providers. This policy outlines the requirements and technical controls that need to be in place prior to entering into a contract with such a provider.

A potential cloud vendor must utilize security best practices, including the following:

- Having a firewall in place
- Restricting data access based on least-privilege principles
- Implementation of account-lockout controls for admin accounts
- Routine audits of account access and privileges
- Collect and routinely review applicable access logs

Additional requirements include, but are not limited to, the following:

- FAU must retain all ownership of data housed on the cloud.
- Transmission of data between FAU and the cloud vendor must be encrypted.
- In the event of contract expiration, termination, or non-renewal, the vendor will return or destroy all FAU-owned data, at the option of FAU.
- Cloud service providers must notify FAU about any data breach within 30 days. For data covered by F.S. 817.5681 or F.S. 501.171, the vendor must notify FAU of any data breach within 10 days. For data covered by FERPA, notification must occur within 72 hours.
- If data being stored with the cloud provider is regulated by FERPA, HIPAA, PCI, or other statutory or regulatory compliance authorities, FAU's Office of the General Counsel and Office of Information Security must be informed to confirm that appropriate contract language is included and special data-handling requirements are satisfied.

### PROCEDURES:

Cloud service providers are required to complete an appropriate assessment tool as provided by the Information Security Officer called the Educause Higher Education Cloud Vendor Assessment Tool (HECVAT) or other applicable assessment tool approved by the Director of Information Security. This assessment references many security controls (like the ones listed above) in order to gauge the security posture of the cloud vendor. HECVAT has a regular form for medium- to high-risk data and a lightweight version for low-risk data. Contact FAU's Office of Information Security (OIT) for assistance if you are unsure of your data's classification and/or which form to provide to the cloud service provider. Completed HECVATs must be submitted to OIT for review and approval prior to any contractual agreements.

University Procurement or OIT may be contacted for assistance with the procurement or approvals for cloud service providers and/or to obtain information on current FAU-approved providers.

### **SANCTIONS:**

Violations of the policies and laws described herein by an employee are grounds for disciplinary action up to and including termination in accordance with applicable University and the Florida Board of Governors regulations and/or collective bargaining agreements. Such disciplinary actions may also include reprimand or suspension. Violations of these policies and laws by any users are grounds for terminating their use of University technology resources and other appropriate sanctions.

Disciplinary or other action taken by the University does not preclude the possibility of criminal charges, as appropriate. The filing of criminal charges similarly does not preclude action by the University.

### **RELATED INFORMATION:**

NIST Special Publication 800-145 (The NIST Definition of Cloud Computing)

# **INITIATING AUTHORITY:**

Associate Provost and Chief Information Officer, Office of Information Technology

POLICY APPROVAL (For use by the Office of the President)	
Policy Number: _12.9	
Initiating Authority Signature:	Date:
Name: Jason Ball	Date
Policies and Procedures Review Committee Chair Signature:	Date:
Name: Elizabeth Rubin	
President Signature:	Date:
Name: Dr. John Kelly	

Executed signature pages are available in the Office of the General Counsel