Subject: **Information Security**	Page **1 of 7**	Policy # Version: 1.1
Title: **Cloud Services Policy**	Revision of: Version 1.0, 6/1/17	Effective Date: **7/11/17**
		Removal Date:

I. PURPOSE

The rapid evolution of cloud computing provides significant advantages to research organizations such as the Feinberg School of Medicine (FSM). Cloud computing can empower our research colleagues and often provide cost advantages over traditional methods of software or computing use. As more companies choose to provide their services through cloud models, it is increasingly clear that there are minimal or no on-premises software alternatives to complete specific computing tasks.

While FSM embraces the evolving cloud computing ecosystem and strives to provide services as rapidly as possible, use of cloud services (such as Amazon Web Services, Microsoft Azure, or Google Apps) for storing or processing data normally maintained on premises reduces visibility and control over proper handling of the data, introducing unique risks that grow in complexity as the consumer is offered greater control of computing resources, and requiring great care be taken to ensure FSM maintains its information security posture.

This policy provides a list of security requirements governing the use of cloud services at FSM, as well as additional safeguards that should be followed when leveraging Infrastructure as a Service (IaaS) platforms. Safeguards are vendor agnostic and intended to leave a degree of flexibility in how they are implemented while proactively managing the risks introduced by using such services.

II. POLICY STATEMENT

The following are required for use of all cloud services at FSM:

1) Cloud services used to store, transmit, or collect personally-identifiable health information will be reviewed and approved prior to implementation by the FSM Deputy CIO and/or the FSM Chief Information Security Officer.

2) For research subject to NU IRB approval a data security plan will be the mechanism through which cloud services will be reviewed and approved.

3) All data must be stored and managed according to NU and FSM policy and applicable regulations; use of third-party providers does not transfer liability.

4) All cloud services must be managed and implemented in accordance with NU-approved vendor contracts and Business Associate Agreements.

5) Failure to follow these policies and standards will lead to sanctions, up to and including administrative suspension of NetID, loss of faculty appointment, department or unit financial penalties, or dismissal from NU.

6) Any consideration of the use of new IaaS services, regardless of type of data stored, must include involvement by FSM IT. Adoption must be approved in advance by FSM Deputy CIO and/or the FSM Chief Information Security Officer, and led and managed centrally by FSM IT.

7) FSM IT will manage IaaS services centrally, ensuring a minimum level of platform security, and acting as an intermediary to provide standard platform templates or preconfigured instances that the customer may provision on a self-service basis (see definition of Managed IaaS).

8) In cases where the requirements in this document cannot be met due to technical, contractual, or logistical limitations, alternate configuration must be clearly documented and exception granted by FSM CISO.

III. PROCEDURE STATEMENT

FSM IT must maintain the following minimum security controls for any production use of IaaS services at FSM:

Request Process

1) Establish and document a request workflow which:
a. Includes initial assessment of needs and information gathering by FSM IT
b. Documents approval by FSM IT leadership
c. Requires and documents training regarding proper use of the service (e.g., hands-on or through vendor videos)
d. Includes formal acceptance of risks and agreement by the customer to follow acceptable use (see form at end of policy)

Access Control

2) Establish and test procedure for granting, revoking, and auditing access to cloud resources and data, which:
a. Achieves alignment with all NU / FSM policies
b. Uses NetID authentication (or centrally managed Active Directory accounts for privileged access)
c. Functionally mirrors existing workflows for provisioning and de-provisioning on-premises resources
d. Follows principle of least privilege relating to which of the Cloud Service Provider (CSP) components are available to the customer to use without intervention by FSM IT (i.e., self-service features)
e. Provides logical containerization of provisioned resources in the management console, to prevent one customer from modifying or accessing another customer's instances or data
f. Prevents customer from modifying security settings
g. Ensures that, should data from the cloud service flow to NU business partner (e.g., NM) or sponsor systems, NU is not in violation of the third party's requirements or any contracts by using the cloud service and that approved data sharing agreements are in place.

3) Enforce password and login policies that meet or exceed the requirements of current NU policies and requirements.
4) Configure multifactor authentication (MFA) for all management console accounts, and prevent customers from being able to disable MFA for their own management console accounts.
5) Restrict remote login to instance Operating Systems according to existing NU and FSM policies, and at a minimum only allow login from FSM/NM networks or NU VPN.

Network Security

6) Configure network segmentation, security zones, and ingress/egress filtering to match rules configured for on-premises datacenters or virtual datacenters.
7) Create or update existing documentation to describe cloud implementation architecture and data flows, including dedicated connections to, and dependencies with, public internet or on-premises systems/services.

Storage Security

8) Encrypt all at rest data with industry standard encryption methods, and securely store encryption keys in a manner that prevents key access by the CSP.

Logging

9) Configure logging capabilities which stores log data to a central location, and includes:
a. Operating System logging that meets or exceeds NU policy and HIPAA requirements, and restricts customer's ability to access/modify logs.
(see http://www.it.northwestern.edu/policies/serversecurity.html)
b. Captures at least 90 days of network activity entering or exiting FSM cloud networks.
(see http://www.it.northwestern.edu/policies/firewall.html)
c. Management console account session activity, modification of security-related configuration items, and provisioning or modifying instances and storage.

Threat & Vulnerability Management

10) Configure vulnerability scanning for all instances under FSM that sends reports and alerts to FSM IT Infrastructure staff and FSM CISO.
11) Ensure all instances are centrally patched by FSM IT, including Operating System and server platform software (e.g., database management systems) as defined by existing NU and FSM policies and procedures.
12) Configure all new instances to include FSM standard host-based security software.
13) Include security event monitoring that examines traffic at the border of the CSP and alerts FSM IT Infrastructure staff and FSM CISO if an event or unauthorized access is detected.

Configuration & Change Management

14) Integrate all configuration changes into established FSM change management process.

Legal / Regulatory

15) Confirm and ensure provisioned resources exist only in US-based virtual datacenters/regions.
16) Define and test a deprovisioning process that maintains data and metadata according to NU data retention policy.
17) Define and test a process for forensically preserving data and metadata intact should it be placed under legal hold.

Business Continuity & Disaster Recovery

18) Configure all instances and storage with redundancy, and establish and test a procedure, that allows service recovery in the event that:
a. An individual service region in the CSP becomes unavailable.
b. The entire CSP becomes unavailable.
19) Configure data backups to match or exceed existing FSM backup procedures, including offsite rotation outside the CSP.

IV. PERSONS AFFECTED:

All NU Feinberg School of Medicine faculty, staff, students, residents and fellows.

V. DEFINITIONS:

Customer

An individual given an account within cloud service by FSM IT, with the privileges to provision resources without intervention by FSM IT staff.

Infrastructure as a Service (IaaS)

Cloud service model as defined by National Institute of Standards and Technology (NIST), wherein the cloud consumer (in this case NU Feinberg School of Medicine) is responsible for provisioning and configuring fundamental computing resources.

Managed IaaS

The IaaS delivery model FSM IT uses, wherein full control of IaaS services is restricted, and FSM IT provides the customer a collection of instances or services preconfigured by FSM IT. These services may then be provisioned by the customer on an on-demand, self-service basis, with the customer being charged for the resources used.

Instance

Virtual server provisioned through IaaS provider.

Management Console

The interface by which customers or IT staff provision or manage cloud services.

Management Console Account

Any account used to access management console functions.

VI. POLICY UPDATE SCHEDULE:

Policy review to occur no less than annually.

VII. REVISION HISTORY:

6/1/17 – New policy effective.
7/11/17 – Vendor contract and Business Associate Agreement requirement added.

VIII. RELEVANT REFERENCES:

National Institute of Standards and Technology (NIST) Definition of Cloud Computing:
http://dx.doi.org/10.6028/NIST.SP.800-146

OpenCrowd Cloud Taxonomy:
http://cloudtaxonomy.opencrowd.com/static/cloudtaxonomy/pdf/cloud_taxonomy_arch.pdf

NU Data Access Policy:
http://www.it.northwestern.edu/policies/dataaccess.html

FSM General Security Policy:
http://www.feinberg.northwestern.edu/it/docs/General-Security-Policy-092216-V2-1.pdf

Secure IT at Northwestern:
http://www.it.northwestern.edu/security/index.html

NU IT Policies:
http://policies.northwestern.edu/policies-by-category.html

HHS Guidance on HIPAA & Cloud Computing:
https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Feinberg School of Medicine Infrastructure as a Service (IaaS) Agreement

Request:
The undersigned will be provided an account within the FSM IaaS environment indicated below, and granted the ability to provision resources through the aforementioned account.

While IaaS services provide a number of advantages over traditional computing services, these advantages come with less control by FSM. This introduces increased risk of data corruption, loss, or unavailability, and the potential for excessive or unintentional charges being assessed for resources used.

Policies:
NU IT Policies: http://www.it.northwestern.edu/policies/index.html
FSM IT Policies: http://www.feinberg.northwestern.edu/it/policies/information-security/index.html

Agreement:
The undersigned understands and accepts the risks as explained in this document, agrees to comply with all requirements listed in this document, and abide by NU and FSM acceptable use policies.

- Account will be carefully safeguarded and not used for shared access under any circumstances.
- Resources will be provisioned carefully to avoid unnecessary charges, and the undersigned will be accountable for payment of all charges assessed.
- No security-related settings in the management console will be modified without approval from FSM IT.
- Application software will be kept up to date with the latest patch levels. FSM IT will provide patching and security for the Operating System.
- Application passwords will be composed per the requirements of Northwestern University IT Policy. http://www.it.northwestern.edu/netid/password.html

Exceptions: (please indicate approved exceptions):

_____

IaaS Cloud Service Provider (e.g., AWS, Azure): _____

Chart String / Purchase Order #: _____

Approved Services (e.g., EC2, S3): _____

Classification of Data (see NU Data Access Policy): _____

NU IRB Number (if applicable): STU_____

Signed: _____

Print Name: _____

Department: _____

Date: _____