NU Cloud Terms of Service

Overview

This document represents the Terms of Service among Northwestern Information Technology (IT) and participating tenants in the NUCloud private cloud environment at Northwestern. The goal of these Terms of Services is to establish a more structured relationship among the participants for management of the technology infrastructure and virtual server resources allocated to the tenants.

Roles

Participants in NUCloud align to one of two roles: Service Provider and Tenant. Northwestern IT acts as the Service Provider for NU Cloud; school and unit participants act as Tenants.
The participants are jointly accountable for:

- Ensuring the NU Cloud is deployed and maintained in accordance with anticipated future direction for Northwestern private cloud.
- Implementing controls to ensure compliance with all University IT-related security policies and applicable regulations.
- Ensuring transparency of planning, implementation, and maintenance of the infrastructure and virtual datacenter use for decision-making.

Service Provider Responsibilities

The Service Provider is responsible for implementing and maintaining NU Cloud infrastructure, including both hardware and software, specifically VMware vSphere. The resulting infrastructure has expected availability equivalent to the existing Northwestern IT virtual server environment.

Specific responsibilities for the Service Provider include:

- Determining new tenants for NU Cloud, in accordance with the Tenant Application process.
- Setting up and configuring virtual datacenters (vDCs) for tenants, including:
  - Handoff of vDC administration and associated access privileges.
  - vDCs are individual to the tenant (Resources and data are not shared among tenants).
- Monitoring the NUCloud infrastructure and underlying systems for availability and performance.
- Maintenance and upkeep of hardware and software components of each pod, keeping software versions no more than one version behind what is currently available.
- Configuring appropriate security mechanisms for the physical and underlying infrastructure, to protect University services and data against malicious activity and to ensure compliance with applicable regulations.
- Ensuring the infrastructure is resilient in the event of server or component failure.
- Providing capabilities for virtual machine (VM) level restores in case of loss or corruption.

Tenant Responsibilities

Each tenant is responsible for its designated virtual datacenter (vDC) and all virtual machines hosted therein. The tenant is expected to ensure service availability to its constituency in accordance with pre-defined service levels.

Specific responsibilities for the Tenant include:

- Monitoring the virtual datacenter and health of resident virtual machines.
- Maintenance and upkeep of virtual machine operating systems and applications (Including Patching to maintain adequate and up to date security levels).
- Ensuring critical services are resilient at the application layer, as appropriate.
- Configuring appropriate VM-based security mechanisms to protect University data against malicious activity.
- Where applicable, establishing business practices that comply with regulatory or research requirements (e.g. HIPAA/HITECH).
- Managing restoration of files or VMs to the tenant's vDC, either through Northwestern IT operated or other defined mechanisms (refer to Service Provider responsibilities), including CrashPlan PRO.
- Archiving critical data that must persist beyond Service Provider's data protection measures, understanding the Veeam backup service is not meant for long-term data archive.
- Ensuring server administrators are appropriately trained and prepared to manage the vDC and servers housed therein. Please be aware Northwestern IT is not staffed to provide vDC or virtual machine administration in the absence of tenant capabilities.

Hosted Data

Tenants are responsible for managing data access, retrieval, storage, and security. NU Cloud may be used in accordance with the data classifications in the Northwestern University Data Access Policy (http://www.it.northwestern.edu/policies/dataaccess.html).

Service Levels

The NU Cloud infrastructure has expected availability equivalent to the existing Northwestern IT virtual server environment. While NU Cloud does not have a specific level of availability defined, it does include the following characteristics for consideration:

- The environment is managed as an administrative system, using data center capabilities such as generator power in the event of a power failure.
- The environment includes redundant components where appropriate, though the design may include single points of failure.
- The intent of NU Cloud is to provide Infrastructure as a Service (IaaS); therefore, any systems and data running in it are solely managed by the tenant. Any system for which Northwestern IT system administration or database administration support is needed should not reside in the NU Cloud, but rather should be part of the Northwestern IT Virtual Server Hosting Services.

NU Cloud also differs from the Northwestern IT Virtual Server Hosting Services; the following table outlines these differences in service levels.

NU Cloud Service Levels

Area	NUCloud	Northwestern IT Virtual Hosting Service
Network	Each tenant has their own subnet(s) and must manage their own IP addresses.	Shared subnets with other DC services.
Firewalls	Tenants in NUcloud3 will have their own Juniper vSRX Firewall appliance and will maintain their own Firewall policies.	Subnets are secured by the Data Center Firewall. Firewall requests are made by Northwestern IT Staff and administered by TNS.
Servers/Services	Servers/services deployed and managed by the tenant. Security, Users and applications configured by tenant. Northwestern IT does not have access to self-deployed servers	Servers deployed by Northwestern IT, day-to-day administration done by either Northwestern IT or System Owner. Northwestern IT retains Administrative/root level access to the servers.
Veeam backups	File restoration requires entire VM to be restored and tenant is responsible for retrieving needed files from restored Virtual Machine.	Since Northwestern IT has system level access, individual files can usually be restored without entire VM being restored.
VM Management	Limited functionality available to tenants for “on the fly” changes to vCPU, RAM, and storage.	Northwestern IT can add and expand storage In some cases. Depending on the OS, can add and remove RAM and CPU hot

Acceptable Use

Tenants agree to comply with applicable University policies (http://policies.northwestern.edu) on the use of information technology resources, security policies, and applicable regulations. Data hosted in NU Cloud, and the management procedures governing that data, must comply with relevant University policies and guidelines, and applicable regulations.

Tenants agree to not host services within NU Cloud that are redundant or conflict with existing Northwestern-provided services. For example, NU Cloud should not be used to host a competing Exchange or SharePoint service.

Security

The NU Cloud infrastructure is housed in Northwestern IT data centers, which have security safeguards in place in accordance with HIPAA/HITECH regulation. Web-based administration transmissions are all SSL-encrypted.

Tenants are responsible for the security of data stored on and transmitted to/from their VMs, and for business practices required of regulatory compliance and research projects, where applicable.

Backups

Full back up of virtual machines for disaster recovery is included in the service and is administered by Northwestern IT. Data may be restored up to 28 days after backup. Up to 48 hours may be needed to restore data from backups older than seven (7) days. In the future, it may become possible for tenant administrators to restore individual files or machines from these backup images; however, the current environment limits restores to Northwestern IT administrators. Tenant administrators may request restores through Northwestern IT, or may choose other backup/restore options such as the central CrashPlan PROe backup service (http://www.it.northwestern.edu/dss/backup-service/index.html).

Please be aware that data protection services used for enterprise applications are not available in NU Cloud. Tenants who have applications that require such data protection should contact Northwestern IT to arrange for appropriate protection measures.

Disaster Recovery

Under this agreement, all parties understand and agree that the infrastructure does not offer resiliency in the event of a site failure at the Evanston Data Center. In the event of such a failure during the term of this agreement, Northwestern IT will coordinate restoration of services with tenants. Prioritization of such restoration will be determined by the University administration as part of the overall event triage and management.

FY 2017 Hosting Fees/Payment

Storage	Size			Additional Compute CPU and RAM	Additional Data/Protection Storage
	Small	*Medium*	*Large*		
Bundled Unit of vCPU, RAM	9	18	24		
CPU (GHZ)	8.96	17.92	23.81	1	
RAM (GB)	90	180	240	10	
Total Storage (TB)	2	3	5		1
Payment Options					
Two Year Pre-Payment	*$4,338*	$7,842	$11,265	$298	$834

Annual Payment	$2,169	$3,921	$5,633	$149	$417

Subscription

Tenants commit to a two (2) year term from the date of access to the vDC. The term will automatically renew each year after the initial term.

This agreement is intended to be reviewed on an annual basis by designates of the Infrastructure Advisory Committee (IAC). It should also be reviewed in the case of staff turnover or upon a request by any party.

Tenants are notified each February of the pending annual renewal. Should a Tenant decide not to renew their tenancy, they have until June 1 to respond in writing. No response by the Tenant automatically renews tenancy for another year.

Adding Additional Capacity

Additional capacity of Compute (Ghz and RAM) and/or Storage may be added to an existing vDC at any time. Capacity may take up to 90 days to deploy, depending on the existing inventory pool of available resources. If resources are available, deployment will occur within 72 hours of request. Capacity can be added in the following increments:

- Compute – 1 Ghz CPU and 10MB of RAM
- Storage – 1 TB of storage

Payments for additional capacity will be billed in July or September of each fiscal year.
Capacity added during the first three quarters of the year will be billed the amount for an entire year. Capacity added in the final quarter of a year will be billed only for the following year and onward.

Termination of Services

The Service Provider and Tenants may jointly terminate this agreement if a more comprehensive technology environment and governance structure is available and it is agreed to move to that structure.

If performance fails to meet partner expectations, the Service Provider and Tenants will meet to review the situation and may terminate the agreement based on available remediation options.

Prior investments made by tenants will not be refunded.

No provision exists for the transfer of remaining investments to another school or unit.

Disposition of Data

The Tenant will have until 30 Days after agreed upon account termination to remove all data from the vDC.

30 days after account termination, all access to the vDC will be terminated, and any remaining Tenant data will be deleted, including backups captured by Veeam.

Removal of content is entirely the Tenant's responsibility.
Service Provider will provide no additional assistance unless mutually agreed upon.

Notifications to Client

Tenants will be notified of any changes to service, outages (planned and unplanned), and security-related issues by Northwestern IT. In general, notifications will be conveyed using existing mechanisms, including the Northwestern IT Service Status website (http://service-status.northwestern.edu/) and associated emails.

In the event of an NU Cloud service issue which impacts multiple tenants or multiple servers or services:

- The IT Support Center will be notified and requested to escalate the issue as critical.
- The tenant-defined point of contact will be reached by Northwestern IT via phone or text message to confirm receipt of the outage notification.
- Northwestern IT will manage the incident using the existing Incident Management procedure. A Major Incident Manager will be defined to engage and follow that process.
- During the outage, the Major Incident Manager will offer updates through the following mechanisms:
    - Stakeholder conference bridge - hourly updates
    - Technical conference bridge – NU Cloud support staff from Northwestern IT and schools/departments where applicable.
    - Comp-Announce and/or other tools to notify community
- After services are restored, Northwestern IT will conduct a root cause analysis and share the resulting report with tenants.

Client Support

The Northwestern IT Support Center (http://www.it.northwestern.edu/supportcenter/index.html) serves as the conduit for tenant support. When contacting Northwestern IT in an emergency situation involving NU Cloud:

1. Call 847-49**1-4357** (1-HELP) option 7.
2. After identifying yourself and your organization, assert you are an NU Cloud tenant and need to speak to the on-call PIPS Infrastructure Engineer in Processing and Information Platform Services.