RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.2.18

Section Title: Legacy UMDNJ policies associated with Information Technology

Policy Name: Server Life Cycle Management

Formerly Book: 95-01-11-01:01

Approval Authority: Vice President for Information Technology & Chief Information Officer

Responsible Executive: Vice President for Information Technology & Chief Information Officer

Responsible Office: Office of Information Technology (OIT)

Originally Issued: 9/8/2009

Revisions: 7/20/2012; 7/1/2013

Errors or changes? Contact: oitpolicy@rutgers.edu

1. **Policy Statement**

This policy is designed to insure that all Rutgers, the State University of New Jersey, servers are maintained and operated in a safe and effective fashion. This is achieved by routine monitoring, timely updating, and eventual decommissioning of the servers. In addition, backup procedures (appropriate for disaster recovery and compliance with applicable laws and policies) must be routinely performed.

2. **Reason for Policy**

To ensure a stable computing environment by specifying the requirements to be followed by all those concerned for the procurement, implementation, management, administration, and decommissioning of servers.

3. **Who Should Read This Policy**

This policy applies to any individual responsible for the management, operation, and/or maintenance of the legacy UMDNJ information technology services and/or environment. If you are uncertain whether this policy applies to you, please contact your direct supervisor.

4. **Related Documents**

Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 (HIPAA)
http://www.hhs.gov/ocr/privacy/index.html

5. **Contacts**

oithelp@rutgers.edu

6. **The Policy**

70.2.18 SERVER LIFE CYCLE MANAGEMENT

I. Requirements:

There are four phases of a server's life cycle, and each phase has its own requirements. This policy requires adherence to all four phases when deploying a server in the Rutgers network environment. Each requirement is independent, and all must be followed. In the event that one requirement has not been met, the remaining requirements of the policy must still be met.

A. Procurement

Make a formal request for service from the Office of Information Technology (OIT) by completing a Project Service Request (PSR) form and submitting it to the appropriate Group or to the OIT Project Management Office (PMO). The PSR form and the Rutgers Project Request and Evaluation policy are available from OIT PMO.

1. The appropriate IT group will create an issue tracking number, referencing the PSR.

2. The appropriate IT group will conduct a needs assessment and coordinate with the requester. It is important that the needs assessment include all interested parties from the requester group, from OIT and from vendors.

3. Needs assessment will include requirements with respect to the following:

   a. Network

   b. Environmental (power, cooling, space, location)

   c. Load and capacity (processor, memory, storage)

   d. Software

   e. Hardware option: new, repurposed, or virtual

   f. Security – sensitive electronic information, HIPAA, access controls.

4. At a minimum, needs assessment will include review of the following topics:

   a. Potential impact on existing systems and infrastructure

   b. Hosting or co-hosting options

   c. Life cycle expectations

d. System(s) management – Details with respect to: patching, backups, disaster prevention and recovery, continuity plans, and application maintenance

e. Vendor involvement; external or internal hosting

f. Support contracts.

5. The appropriate IT group will take action as detailed in OIT's Project Request and Evaluation policy:

a. Estimate the hours and costs for implementation

b. Review the estimate with the requester and then with the appropriate IT group.

c. Determine project management and team participation requirements.

6. Servers must be purchased in accordance with the University's Purchasing Process policy. The appropriate IT group will assist procurement as necessary.

B. Implementation

1. There must be a documented procedure to ensure that servers are built in a consistent configuration with respect to platform, system, and system hardware for the appropriate IT group. This documented procedure must address the minimum configuration standards listed below, in section **IC5** on Management and Administration.

2. Servers must be located in a safe environment. At a minimum, a safe environment provides shelter from the elements, temperature modulation, reliable power, fire system and limited physical access. Further, University policy, Protection of Sensitive Electronic Information (SEI), requires that:

a. Physical access to the University data control centers shall be controlled by an appropriate authentication or access mechanism. This access system shall be monitored and maintained by Public Safety.

b. The Physical Plant Department shall be responsible for the maintenance of the following security-related physical components of University facilities: a. defective doors, hinges, and closers; b. broken window units and glass; c. damaged interior and exterior walls.

c. Public Safety shall be responsible for maintenance of the security-related physical components of University facilities related to keys, locks, doorknobs, push bars, and latches.

Finally, each campus or data center may have additional physical requirements that must be documented by the appropriate IT group and followed at this step.

3. All servers must be registered using appropriate server registration processes.

4. Rutgers OIT must be notified of the installation of the server in accordance with the University policies.

5. Server security must be established and documented. Server hardware, software, applications and respective data access must be controlled, restricted, and secured at the time of implementation. A best-effort attempt must be made by the server administrator to identify, document and mitigate any security risks. In addition, the server administrator must satisfy any external regulatory requirements and any Rutgers applicable policies, for example:

    a. Public Law HIPAA dictates that it is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure.

C. Management and Administration

1. Server hardware, operating systems and applications must be maintained and managed on a routine basis to ensure that they are available during normal hours of use and performing satisfactorily per recommended specifications.

2. A procedure must be established and documented, or OIT services obtained, to upgrade and patch the operating system, drivers, firmware, and any hosted applications. When a manufacturer or vendor withdraws support for a product, it should be replaced. If replacement is not possible, the procedure for maintaining obsolete systems should be followed.

3. A procedure must be established and documented to ensure the server is secure, based on the regulatory laws or policies governing the application and data hosted by the server. Logs containing user access information must be reviewed at least once before they are overwritten, with a maximum of three months between review periods. A best-effort attempt must be made to establish and document a method to validate access.

4. A procedure must be established and documented to backup server-hosted data. Backups must be scheduled on a recurring basis. A procedure must also be established and documented to retain backup copies of server-hosted data. Schedules for backups and retention periods must take into account the regulatory laws or policies governing the application and data hosted by the server as well as the University, school or unit disaster recovery and continuity plan.

5. Monitoring procedures must be established and documented, or OIT services obtained, that satisfy all of the server management requirements, including but not limited to application availability, resource availability, patching, security, backups and functional review.

6. Rutgers OIT must be notified of changes to the server in accordance with the University policies.

7. A functional review must be conducted annually to assess the need for the server and its function(s).

D. Decommissioning

1. When the server is no longer required it must be decommissioned.

2. Make a formal request for service from of Information Technology (OIT) by completing a Project Service Request (PSR) form and submitting it to the appropriate OIT department or to the OIT Project Management Office (PMO).

3. The appropriate IT group will create an issue tracking number, referencing the PSR. The issue description must include the following concerns, if applicable:

   a. Unneeded power, cooling, space and network connections

   b. IP reservations, network name registration, network address translations and firewall rules

   c. Application dependencies or references to the server

   d. Unneeded OIT enterprise services, applications or backup processes

   e. Disaster recovery and continuity plan.

4. Data purging procedures must adhere to both Rutgers policies and state retention laws.

5. A procedure must be established and documented to notify appropriate stakeholders including user communities, OIT and local data center if applicable.

6. All servers must be un-registered per OIT policy.

II. Enforcement

A. OIT will enforce this policy.

III. Procedures

The following procedures have been described and are required by this policy:

A. Project Service Request form for procuring and for decommissioning a server

B. Issue tracking number for procuring and for decommissioning a server

C. Needs assessment

D. Cost estimate

E. Purchase documentation

F. Server Registration

G. Initial server configuration, including physical location, hardware, operating system, applications, registration, life cycle requirements, security.

H. Server monitoring, including application availability, resource availability, patching, security, backups and functional review.

I. Change control in the form of submissions to the OIT Change Management Committee

J. Decommissioning procedures including data purging, equipment disposal, service deletion and notification.

K. Server Un-registration.