RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.2.6

Section Title: Legacy UMDNJ policies associated with Information Technology

Policy Name: Network Security Management

Formerly Book: N/A

Approval Authority: Senior Vice President for Administration

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

Responsible Office: Office of Information Technology (OIT)

Originally Issued: July 1, 2013

Revisions: Originally 00-01-95-20:10 at UMDNJ; 10/10/2013 (Updated title)

Errors or changes? oitpolicy@rutgers.edu

1. **Policy Statement**
   Appropriate management of Rutgers, The State University of New Jersey, computing resources and the network infrastructure interconnecting them is a critical information security requirement for the University. The underlying IT infrastructure must be designed, procured, deployed, operated and maintained in accordance with good information security principles.

2. **Reason for Policy**
   To ensure the protection of information passing over the University's network (wired and wireless) and the protection of the supporting infrastructure, including applications and other systems that rely on the University's network for business-critical services.

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**
   N/A

5. **Contacts**
   oithelp@rutgers.edu

6. **The Policy**

70.2.6 NETWORK SECURITY MANAGEMENT

The secure management of the University's networks, which may span organizational boundaries, requires the careful consideration of the flow of information and regulatory requirements regarding monitoring and protection.

Networks must be adequately managed and controlled in order to be protected from threats. Network management must also consider how changes to one element of the network or connected resource may impact the security of other University systems and applications using the network, including the confidentiality, integrity, and availability of University information in transit. Office of Information Technology (OIT) is solely responsible for the installation, provisioning, and management of the University's network services and infrastructure.

Confidentiality, Integrity, and Availability must be adhered to when planning, implementing, and managing the University's network resources and infrastructure:

- **Confidentiality** – the expectation that only authorized individuals, processes, and systems will have access to Rutgers' information.
- **Integrity –** the expectation that Rutgers' information will be protected from intentional, unauthorized, or accidental changes. Rutgers' information is relied upon by business-critical functions and processes to accurately process transactions and provide accurate information for decision-making.
- **Availability –** the expectation that information is accessible by Rutgers authorized individuals when needed.

I. Requirements:

A. All University schools/units must adhere to the network security standards defined by OIT.

B. OIT's network managers must define and implement security standards to ensure the security of information transmitted over or outside of the University's networks, and ensure the protection of the University's network-connected services from unauthorized access. This includes security of the University's wired and wireless networks, as well as remote access to the University's network infrastructure. In particular, the following items should be considered:

1. Operational responsibility for the University's networks should be separated from computer operations where appropriate.
2. Responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established.
3. Special controls should be established to safeguard the confidentiality and integrity of University information passing over public networks or wireless networks, and to protect network-connected systems and applications. Special controls may also be required to maintain the availability of the network services and connected computers.
4. Appropriate logging and monitoring should be applied to enable recording of security-relevant actions.
5. Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the University's network infrastructure.

II. Responsibilities:

A. Vice Presidents and Deans: are responsible for ensuring that their school or unit complies with the network security standards defined by OIT. They are also

responsible for ensuring that their personnel do not present an information security risk to the University by introducing devices or information systems that may compromise the confidentiality, integrity, or availability of the University's information technology infrastructure, resources, or services.

B. Information Protection and Security Office: must define the appropriate operational controls necessary to mitigate the risks associated with the unauthorized disclosure, loss, or theft of University information.

C. OIT: must define the network security technical standards that meet the information security requirements of the University, particularly those mandated by regulations and statutes governing the institution.

D. Non-OIT Technology Teams: must adhere to policies established by OIT.

E. Schools and Units must ensure devices they connect to the network are maintained according to OIT standards as per the University's Server Life Cycle Management Policy which defines the requirements for maintaining servers.

III. Non-Compliance and Sanctions

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable state and federal statutes.