RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

# RUTGERS POLICY

**Section:** 70.2.9

**Section Title:** Legacy UMDNJ policies associated with Information Technology

**Policy Name:** Information Security: Remote Access

**Formerly Book:** 95-01-09-01:00

**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:** 7/25/2012

**Revisions:** 7/1/2013

**Errors or changes?** itpolicies@rutgers.edu

## 1. Policy Statement

The policy specifies the requirements and responsibilities regarding remote access to Rutgers, The State University of New Jersey, electronic information and information systems in order to minimize the risks associated with off-campus access to the University's data.

## 2. Reason for Policy

The purpose of this policy is to specify the requirements and responsibilities relative to remote access to Rutgers' electronic information and information systems.

## 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**

## 70.2.9 INFORMATION SECURITY: REMOTE ACCESS

Remote access services are secure network enterprise services provided and managed by Rutgers' Office of Information Technology (OIT) organization to allow authorized users to securely access the University's electronic information and information systems from an off-campus location using a personal computer, mobile computing device, or from a Rutgers-issued laptop. Remote access services are provided exclusively to staff, faculty, and authorized contractors to perform their job duties from a non-campus location.

Remote access services mitigate the risks of 1) lost or stolen electronic information, 2) malicious software being introduced into Rutgers' electronic environment, and 3) unauthorized access to University information systems. All activity, including the saving of information, is conducted over a secure remote session, rather than on the local computer. Therefore, it is Rutgers' preferred method of off-campus access to those University electronic assets.

Staff and faculty who regularly need to access and use Rutgers' electronic assets off-campus should use remote access services rather than use removable media to transport Rutgers' electronic information or forward University electronic information to a personal email account (which is prohibited when working with information classified as Confidential or Private or otherwise treated as sensitive).

Contractors who require remote access to Rutgers' electronic information or information systems must be limited specifically to the electronic information and information systems they need to access in order to fulfill the terms of their contract. Upon termination of the individual's contract or termination of the vendor's contract, remote access services must be terminated.

In order to protect the confidentiality, integrity, and availability of Rutgers' electronic information and information systems, activity may be reviewed, logs captured, and access monitored without notification. Access to remote access services must be reviewed according to the requirements stipulated in the University's Information Security: Electronic Information and Information Systems Access Control policy.

All University policies, standards, procedures, and guidelines that apply to on-campus access to and use of Rutgers' electronic information and information systems are applicable when using non-Rutgers computers (e.g., personal desktop computers and laptops).

Rutgers reserves the right to terminate, without prior notification, an individual's access to remote services if the University perceives there is an immediate risk or threat to Rutgers' electronic information or information services.

### I. Requirements

A. Users must follow necessary processes to request remote access services.

B. When sharing a personal computer with others (such as friends or family members), users must not leave a remote access session unattended.

### II. Responsibilities

C. Users are responsible to give the same consideration regarding privacy and security to their remote access connection to Rutgers' electronic information and information systems as to on-campus use and access to those assets.

D. Managers and Supervisors are responsible for:

1. Notifying OIT when remote access services must be discontinued for a member of their organization, even if the person remains in the employ of Rutgers.

2. Notifying OIT within 24 business hours upon termination of an individual contractor or termination of a vendor’s contract in order to ensure the individual’s (or a vendor’s employees) remote access services are terminated promptly.

3. Following the University’s termination and transfer procedures when a member of their organization leaves the University or transfers to another school, unit or department.

## III. Prohibited Services

Users may not us non-Rutgers approved remote access services to access their Rutgers workstations.

## IV. 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.