RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

**RUTGERS POLICY**

**Section:** 70.2.21

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

**Policy Name:** Information Security: Workstation Use and Security

**Formerly Book:** 95-01-09-03:00

**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:** 8/23/2012

**Revisions:** 7/1/2013

**Errors or changes?** Contact: oitpolicy@rutgers.edu

1. **Policy Statement**

   This policy specifies the appropriate use and security applicable to Rutgers, The State University of New Jersey, workstations. Acceptable workstation use must be defined in order to protect the confidentiality, integrity, and availability of Rutgers's electronic information and information systems.

2. **Reason for Policy**

   This policy specifies the appropriate use and security applicable to Rutgers' workstations.

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**

**70.2.21 INFORMATION SECURITY: WORKSTATION USE AND SECURITY**

Rutgers's workstations are provided by the University for business, academic, and research use. They must be used in accordance with the University's policies and secured against unauthorized access.

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.

I. Requirements

A. Workstation Use

1. Removable Media: Connecting personal removable media, particularly portable hard drives and USB thumb drives, to legacy UMDNJ workstations is prohibited.

2. Users must not save on workstations information classified Confidential, Private, or otherwise considered sensitive or privileged information, unless it is appropriately secured against theft or loss.

a. Users and business units should consult with OIT regarding what kind of security is appropriate for the sensitive information they store on their local workstations.

b. Outlook email archives are automatically stored locally on workstations. If email archives contain sensitive information (in the message body or in an attachment), they must be secured against theft or loss of the workstation.

3. Sensitive information should be saved in folders with access limited to those individuals authorized to access the information.

4. Folder access entitlements must be reviewed according to the University's "Information Security: Electronic Information and Information Systems Access Control policy."

5. Users must logoff or lock their workstations when not in use.

6. Users should consider using a privacy screen to prevent unauthorized people from viewing information on their workstation screen.

7. Users must consult with OIT before installing software or connecting hardware that has not been issued or purchased by Rutgers.

8. When installing personal software authorized by Rutgers, users must provide and retain proof of purchase and licenses (unless the software is offered free by the software developer).

B. Workstation Security

1. Workstation builds must incorporate Rutgers' baseline security controls and safeguards defined by the Office of Information Technology (OIT).

2. Workstations that deviate from Rutgers' baseline security controls and safeguards must be identified. Deviations must be documented and state:

a. The department where the workstation resides.

b. The purpose of the workstation.

c. The workstation's serial number.

d. The controls and safeguards not applied to the workstation.

e. The business justification for deviating from Rutgers' baseline security controls, safeguards, and configurations.

f. The IT manager approving the deviation.

3. IT service organizations and the businesses are expected to maintain an accurate and current inventory of all workstations.

   Login banners are required. Please consult OIT regarding necessary login banner requirements.

4. Idle timeout mechanisms must be employed.

5. A user ID and password must be required to use the workstation.

6. Local workstation administrator access is a privilege and will only be granted when a clear business need is established and standard University IT services or alternative solution cannot support the user's business needs.

   a. The University reserves the right to revoke without notice local administrator privileges if access is deemed to present a risk to Rutgers' electronic information or information systems.

   b. The user's manager and/or the University's IT service organizations will periodically re-assess the user's need for administrator access and at their discretion revoke the entitlement (without notice) or offer an alternative solution to meet the user's need.

   c. Workstation administrator access is auditable and subject to access entitlement reviews.

7. Workstations that provide access to or use of sensitive information or information systems should not be located in publicly accessible areas.

   a. If a workstation must be located in a public area, physical and technical safeguards must be employed to protect against unauthorized access.

   b. When feasible, workstation monitors should face away from public viewing.

II. Responsibilities

A. Office of Information Technology (OIT) is responsible to define base controls and configurations for workstation builds.

B. All Rutgers IT services organizations are responsible to incorporate the University's baseline security controls, safeguards, and configurations into their workstation builds and to maintain an accurate and current inventory of all their workstations. Any deviation from Rutgers' baseline security model must be documented.

C. The President/CEOs and Vice Presidents of the University's units and the Deans of the schools have ultimate responsibility for the protection of their electronic information and information systems against unauthorized disclosure, loss, or misuse. They must ensure that all members of their respective organizations follow the administrative, physical, and technical safeguards defined in this policy.

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.