RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.2.22

Section Title: Legacy UMDNJ policies associated with Information Technology

Policy Name: Information Security: Electronic Information and Information Systems Access Control

Formerly Book: 00-01-95-15:20

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: 4/20/12

Revisions: 7/1/2013; 10/10/2013 (Updated title)

Errors or changes? Contact: oitpolicy@rutgers.edu

1. **Policy Statement**
   Authentication and access control measures should ensure appropriate access to Rutgers, The State University of New Jersey, information and information processing facilities – including mainframes, servers, desktop and laptop clients, mobile devices, applications, operating systems and network services – and prevent inappropriate access to such resources. Administrative, physical, and technical safeguards necessary to manage and control access to Rutgers' information systems must be defined and enforced.

2. **Reason for Policy**
   To establish the access controls necessary to safeguard the University's 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**
   Health Insurance Portability and Accountability Act of 1996
   http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

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

6. **The Policy**

70.2.22 INFORMATION SECURITY: ELECTRONIC INFORMATION AND INFORMATION SYSTEMS ACCESS CONTROL

Access to the University's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, access is governed by law and other University policies.

Persons or entities with access to the University's electronic information and information systems are accountable for all activity associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by the University, irrespective of the medium on which the information resides.

Access must be granted on the basis of least privilege—only to resources required by the current role and responsibilities of the person. In addition to the administrative, physical, and technical safeguards presented in this policy, the security requirements defined in the University's Information Classification policy must be followed.

I. Requirements:

Access controls to the University's information systems must be established to ensure the confidentiality, integrity, and availability of the data accessible via those systems.

A. Registration of Access

With respect to registration of access to the University's information systems:

1. There must be a formal authorization process documented for access requests.

2. The requester's identity must be confirmed and authenticated.

3. User activity must be logged and tied to the user ID provisioned to the user.

4. User IDs must be unique and require a password.

5. Requests for access must be approved by the requester's manager or their delegate.

B. Registration of Access for Non-Rutgers Personnel

1. Individuals who are not members of the Rutgers community and who have a justifiable business reason to gain access to Rutgers information services must go through the guest account registration process.

2. Registration must follow the requirements listed in section 6IA – *Registration of Access.*

C. De-Provisioning of Access

Cancellation of access to all University information systems, facilities, and information services (e.g., remote access) must be done in accordance with the procedures listed in University policy, Cancellation of Access to University Assets.

II. Information System Identity Access Management

A. Information systems must, at minimum, require a user ID and password.

1. Requests for a deviation from this requirement are limited to clinical systems which have been identified by the school or unit as requiring a different access method in order to provide patient care.

2. Deviations must be reviewed and approved by the Vice President for Information Technology of OIT.

B. User ID Naming Conventions

User ID naming conventions must follow OIT standards.

C. Passwords

1. User IDs must have an associated password.

2. Passwords must be configured to follow OIT standards and/or vendors' recommendations for strong passwords.

III. Generic Accounts

A. Generic accounts are subject to the requirements in this policy.

B. The accounts must be restricted to a specific device and named according to the device's naming convention.

C. Generic accounts must be restricted to kiosks or specialty devices where standard authentication may impede the functionality of the device.

IV. Guest Accounts

A. Guest accounts are subject to the requirements in this policy.

B. The accounts must be sponsored by a Rutgers employee who is responsible for the safeguarding of the information or information system as detailed in Section IX – Separation of Duties.

C. The accounts must have a lifecycle no longer than 12 months, after which they must be re-approved by the sponsor.

V. Service Accounts

A. Service accounts are subject to the requirements in this policy.

B. Service accounts can only be created by a member of Rutgers' Active Directory or Domain Administrators team to facilitate an identified operational need.

C. Service accounts do not expire.

VI. System Default Service Accounts

A. Whenever possible, system default service accounts should be renamed or disabled as long as it does not adversely impact the operations of the application or other dependencies.

B. System default Service Accounts do not expire.

VII. Physician Emergency Access Procedures to electronic protected health information (ePHI) Information Systems (HIPAA § 164.312(a)(2)(ii)).

A. HIPAA requires that each school and unit establish documented emergency access procedures for ePHI information systems.

B. The procedures must satisfy the following two requirements:

1. The ability for physicians to access ePHI during a health emergency.

2. A contingency method for physicians to access ePHI if a natural or manmade disaster makes an information system unavailable.

C. Any deviation from HIPAA § 164.312(a)(2)(ii) must be documented and presented to the Office of Ethics, Compliance and Corporate Integrity and the Office of the Senior Vice President and General Counsel.

VIII. Facility Access

A. Physical access to the facilities where information systems are housed must be limited to personnel specifically authorized to access those information systems in the facilities.

B. Access to the University's data centers must be approved by the data center manager and follow the Department of Public Safety's access request process.

IX. Separation of Duties

A. Access requests, authorization, and administrative responsibilities for information classified as Confidential or Private (otherwise considered sensitive) and their associated information systems should be separated.

B. Users should not have access privileges that would permit them to approve their own changes to an information system or electronic record.

C. If separation of duties is not possible due to staffing limitations, other mitigating controls must be in place to reduce the risk of fraud or tampering.

X. Access Entitlement Review

A. Access to information systems with information classified as Confidential or Private, or otherwise considered sensitive, must be, at minimum, reviewed quarterly.

B. Access to information systems with non-sensitive information must be reviewed semi-annually.

C. Access to the University's data centers must be reviewed semi-annually.

XI. Responsibilities

A. President/CEOs, Senior Vice Presidents, Vice Presidents, and Deans:

1. Are responsible for safeguarding their organization's electronic information and information systems.

2. Must ensure that each member of their organization understands the need to protect the University's electronic information and information systems.

3. Must communicate this policy to all members of their organization.

B. Business Unit Management:

1. Are responsible for safeguarding their unit's electronic information and information systems.

2. Must perform and comply with the policy requirements relevant to their position and responsibilities.

3. Must ensure managers reporting to them perform and comply with the policy requirements relevant to their position and responsibilities.

C. Information Owners must:

1. Establish access authorization procedures to their electronic information and information systems.

2. Establish physician emergency access procedures for ePHI information systems they own.

3. Perform and comply with the policy requirements relevant to their information systems.

4. Review access entitlements to their information systems as stipulated in this policy or when requested by OIT, the Information Protection and Security Office, and/or Internal Audit.

XII. 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.