RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.2.23

Section Title: Legacy UMDNJ policies associated with Information Technology

Policy Name: Rights & Responsibilities for the Use of University-Accessed Electronic Information Systems

Formerly Book: 00-01-95-10:05

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: 8/31/1999

Revisions: 1/26/2011; 7/1/2013; 10/10/2013 (Updated title)

Errors or changes? Contact: oitpolicy@rutgers.edu

1. **Policy Statement**
   This policy applies to individuals accessing and using Rutgers, The State University of New Jersey, computing, networking, telephony and information resources through any facility of the University. These individuals include students, faculty, visiting faculty, staff, volunteers, alumni, persons hired or retained to perform University work, external individuals and organizations, and any other person extended access and use privileges by the University under contractual agreements and obligations or otherwise.

2. **Reason for Policy**
   To set policy for the use of the University's electronic information systems, broadly defined, including users' rights and responsibilities.

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**

70.2.23 RIGHTS & RESPONSIBILITIES FOR THE USE OF UNIVERSITY-ACCESSED ELECTRONIC INFORMATION SYSTEMS

I. General Principles:

A. The University owns it's computing, networking, telephony and other communications systems and its information resources, and has the right to monitor them. The University also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The University has the responsibility for the security, integrity, maintenance and confidentiality of the electronic systems.

B. Computing, networking, telephony and information resources of the University, including access to local, national and international networks, exist to support students, faculty and staff as they carry out the education, research, health-care and public-service missions of the University, and its administration and management. Toward these ends, the University encourages and promotes the use of these resources by the University community. Access to and use of these resources for purposes or activities which do not support the University's missions are subject to regulation and restriction to ensure that they do not interfere with legitimate work; and any access to or use of these resources and services that interferes with the University's missions and goals is prohibited.

C. When demand for computing, networking, telephony and information resources exceeds available capacity or resources, priorities shall be established for allocating the resources, with a higher priority to activities essential to the missions of the University. The Deans and Vice Presidents, in conjunction with the Vice President for Information Technology & Chief Information Officer, shall set these priorities.

D. Information owners and system administrators shall develop and publicize specific written procedures to protect the rights of legitimate authorized users, to protect the integrity of the information and systems under their management, and to delineate the responsibilities of users. The University has the authority to control or refuse access to anyone who violates these procedures or threatens the rights of other users or the availability and integrity of the systems and the information. Actions that may be taken under this authority include deactivating accounts, access codes or security clearances; stopping processes; deleting affected files; and disabling access to computing, networking, telephony and information resources.

E. Users' expectation of electronic privacy must be balanced against the University's reasonable need to supervise, control and operate the University's information systems.

F. The University does not archive E-mail that has been sent or received by its systems. The user is responsible for archiving E-mail messages that the user wishes to retain.

II. Rights of Users:

A. *Privacy and confidentiality*: Because the primary use of the University's communications systems is to further the University's missions, members of the University community should not have the expectation of privacy in their communications, whether work-related or personal. By their nature, electronic communications, especially E-mail connected to the Internet, may not be secure from unauthorized access, viewing or infringement. Although the University employs technologies to secure certain categories of electronic messages, as a rule confidentiality of E-mail and other electronic documents cannot be assumed.

The University cannot and does not make any guarantee, explicit or implied, regarding the confidentiality of E-mail and other documents and messages stored in electronic media unless provisions, approved and maintained by the University, are specifically implemented to this purpose. Users should not expect total privacy when using E-mail.

Although the University will not monitor the content of electronic documents or messages as a routine matter, it reserves the right to examine all computer files in order to protect individuals and the University. In addition, during the course of routine conduct of University business, routine management of the University's computing and networking systems, as well as during emergencies, the University has the right to view or monitor users' files, data, messages or other activity for legitimate business purposes, with or without notice to users. Information seen in such a manner will ordinarily be kept confidential, but may under certain circumstances be used in disciplinary proceedings if appropriate. If an individual is suspected of violations of his/her responsibilities as described in this policy or of other misconduct, the University reserves the right to take any and all actions to abide by the law and maintain network integrity and the rights of access of others authorized to use the system. The University also reserves the right to access and disclose messages, data, files, and E-mail back-up or archives, if such exist, to law enforcement authorities and others as required by law, to respond to legal processes, and to fulfill its obligations to third parties. E-mail is subject to legal discovery during the course of litigation, even if deleted, by means of message archives, back-up tapes and undeleting the messages.

Therefore, good judgment dictates the creation only of electronic documents that may become public without embarrassment or harm.

B. *Safety*: Unwanted communications and offensive or objectionable materials are available through the Internet and may be blocked or regulated by the University. The University accepts no responsibility for the content of electronic mail received; however threatening, harassing or offensive communications received by University personnel over the network should be reported to OIT, Public Safety and, if appropriate, to the Office of Institutional Diversity & Equity.

C. *Intellectual freedom:* The network is a free and open forum for the expression of ideas. The University will not prevent expressions of academic opinions on the network as long as these opinions are not represented as the views of the University and are not in conflict with University policies or state and federal laws. Even with disclaimers about not representing the views of the University, appropriate language, behavior and style should still be used in communications distributed on the University's computing and networking facilities. It should be remembered that certain categories of speech–defamation, obscenity and incitement to lawlessness – are not protected by the Constitution. The University reserves the right, at its sole discretion, to decline to post, to remove posted pages or to restrict University Web sites or computer accounts which contain or are used for personal expressions of a non-academic nature.

III. Responsibilities of Users:

A. Individuals with access to the University's computing, networking, telephony and information resources have the responsibility to use them in a professional, ethical and legal manner. Users are required to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting in a manner to maintain an academic and work environment conducive to carrying out the University's missions efficiently and productively. Specifically, responsibilities of users include:

1. Respecting the rights of others, including intellectual property, privacy, freedom from harassment, and academic freedom;

2. Safeguarding the confidentiality of certain information and the privacy of patients;

3. Using systems and resources so as not to interfere with or disrupt their normal operations or their access use and use by others so authorized;

4. Protecting the security of University electronic systems and the integrity of information stored there;

5. Knowing and obeying University and unit-specific policies and procedures governing access and use of electronic systems and of information.

B. Individuals are prohibited from sharing passwords or log-in IDs or otherwise giving others access to any system for which they are not the information owners or system administrators with appropriate authority. Users are responsible for any activity conducted with their computer accounts and are responsible for the security of their passwords.

C. Individuals may not use another person's network account or try to obtain password or access code to another's network account to send or receive messages.

D. Individuals must identify themselves and their affiliation accurately and appropriately in electronic communications and may not disguise the identity of the network account assigned to them or represent themselves as someone else.

E. The University's communications systems may not be used to harass, intimidate, threaten or insult others; to interfere with another's work or education; to create an intimidating, hostile or offensive working or learning environment; or to conduct illegal or unethical activities.

F. The University's networks may not be used to gain or attempt to gain unauthorized access to remote networks or computer systems.

G. Individuals are prohibited from deliberately disrupting the normal operations of the University's computers, workstations, terminals, peripherals or networks.

H. Individuals may not run or install on any University computer system a program that may result in intentional damage to a file, or that may intentionally compromise the integrity of the University's systems or the integrity of other computing environments via the University's network (e.g., computer viruses, Trojan horses, worms or other rogue programs).

I. Individuals are prohibited from circumventing access and use authentication systems, data-protection mechanisms, or other security safeguards.

J. Individuals must abide by all applicable copyright laws and licenses, and respect other intellectual-property rights. Information and software accessible on the Internet is subject to copyright or other intellectual-property-right protection. University policy and the law forbid the unauthorized copying of software that has not been placed in the public domain and distributed as "freeware." Therefore nothing should be downloaded or copied from the Internet for use within the University unless express permission to do so is stated by or received from the

owner of the material, and the owner's requirements or limitations on use of the material are observed. The use of software on more than the licensed number of computers, unauthorized installation of unlicensed software on University computers, plagiarism and invasion of privacy are also prohibited. "Shareware" users must abide by the requirements of the shareware agreement.

K. Activities that waste or unfairly monopolize computing resources (such as unauthorized mass mailings; electronic chain letters, junk mail and other types of broadcast messages; unnecessary multiple processes, output or traffic; exceeding network directory space limitations; excessive game-playing or other trivial applications; and excessive printing) are prohibited.

L. Reading, copying, changing or deleting programs or files that belong to another person or to the University without permission is prohibited.

M. The University's computing resources may not be used for commercial purposes or personal financial gain.

N. All network communications exiting the University are subject to the acceptable-use policies of the network through which they flow.

O. Use of the University's systems that violates local, state or national laws or regulations or University policies, standards of conduct, or guidelines is prohibited.

P. Confidential information should be encrypted before transmission over open public networks such as the Internet, or such transmission should only be over secure dedicated lines. Including confidential University information in unencrypted E-mail is forbidden.

IV. E-mail and other electronic communications (Internet services, voice mail, audio- and video-conferencing, and facsimile messages):

A. The use of University resources for electronic communications must be related to University business, including academic pursuits, and not for personal or commercial purposes, except for incidental and occasional personal non-commercial use when such use is clearly insignificant, does not generate a direct cost for the University, and does not interfere with or compete with legitimate University business.

B. Only authorized persons may use the University's electronic communications systems.

C. Electronic communications whose meaning, transmission or distribution is illegal, unethical, fraudulent, defamatory, harassing or irresponsible are prohibited. Electronic communications should not contain anything that could not be posted on a bulletin board, seen by unintended viewers, or appear in a University publication. Material that may be considered inappropriate, offensive or disrespectful to others should not be sent or received as electronic communications using University facilities.

D. Appropriate standards of civility and decency should be observed in electronic (as well as all other forms of) communication.

V. World Wide Web:

A. "Official" University Web pages are those that provide information about established, University-recognized entities, such as its Schools; patient-care

units; administrative offices; research institutes, centers and programs; educational programs; clinical centers, institutes and programs. Information on official University Web pages represents the institution and therefore must be accurate, timely and useful and must conform to this and all other University policies, standards and requirements. Official Web pages shall be held to the same standards as any University, school or unit printed publication.

1. The pertinent Dean, Vice President or Department Chair has the ultimate responsibility for official Web pages. These individuals or their designees must authorize the establishment of any official Web page under their purview.

2. The University logo must appear on all official Web pages, or their equivalent.

3. Official Rutgers Web pages shall be reviewed by the responsible party every six to twelve months and these reviews documented by changing the revision date at the bottom of the page.

4. Official Rutgers Web pages may be copyrighted. Official Rutgers Web pages should not contain copyrighted materials without appropriate copyright permission.

B. Faculty professional Web pages and personal Web pages of a faculty member, student or staff member *may not:* promote illegal activities; harass anyone inside or outside the University; include offensive or objectionable material or language or link to other sites that do; distribute copyrighted materials; be used for commercial purposes or personal gain unrelated to the University's missions; contain the University logo; represent the contents as being the official policy or positions of the University. Personal pages from individuals or groups must include the identity of the author, and should contain the following statement: "*The views and opinions expressed in this page are strictly those of the author. The contents have not been reviewed or approved by Rutgers, The State University of New Jersey."* The University reserves the right to not post or remove posted pages for any reason.

VI. 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.