RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS POLICY

Section: 70.1.1

Section Title: Information Technology

Policy Name: Acceptable Use Policy for Computing and Information Technology Resources

Formerly Book: N/A

Approval Authority: Senior Vice President for Finance and Administration

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

Responsible Office: Office of Information Technology (OIT)

Originally Issued: N/A

Revisions: 8-30-2001

Errors or changes: Contact: **itpolicies@rutgers.edu**

1. **Policy Statement**
   This policy outlines the standards for acceptable use of university computing and information technology resources, which include, but are not limited to, equipment, software, networks, data, and stationary and mobile communication devices whether owned, leased, or otherwise provided by Rutgers University.

2. **Reason for Policy**
   Preserving access to information technology resources is a community effort which requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the standards established here for acceptable use.

3. **Who Should Read Policy**
   All members of the Rutgers University community

4. **Related Documents**
   Identity Theft Compliance Policy http://policies.rutgers.edu/PDF/Section50/50.3.9-current.pdf

   Copyright Policy http://policies.rutgers.edu/PDF/Section50/50.3.7-current.pdf

   RU Secure Website http://rusecure.rutgers.edu/

   New Jersey Identity Theft Prevention Act, NJSA 56:8-161 through 56:8-166, http://www.njleg.state.nj.us/2004/Bills/PL05/226_.HTM

   Family Educational Rights and Privacy Act (FERPA), http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

New Jersey Public Access to Government Records Law P.L. 2001, Chapter 404, as incorporated in NJSA 47:1A-1 et seq.
http://www.njleg.state.nj.us/2000/Bills/PL01/404_.HTM

Amendment to the Federal Rules of Civil Procedure
http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

5. **Contacts**

Information Protection and Security, OIT
732-445-8011
rusecure@rutgers.edu

6. **The Policy**

A. Introduction

It is the policy of Rutgers University to maintain access for its community to local, national and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nevertheless, Rutgers reserves the right to limit or restrict the use of its computing and information technology resources based on applicable law, institutional policies and priorities, and financial considerations. Access to the university's information technology resources is a privilege that requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable use.

This policy outlines the standards for acceptable use of university computing and information technology resources, which include, but are not limited to, equipment, software, networks, data, and stationary and mobile communication devices owned, leased, or otherwise provided by Rutgers University.

This policy applies to all users of Rutgers computing and information technology resources. This includes but is not limited to, faculty, staff, students, guests, and external individuals or organizations.

B. User Responsibilities:

1. **Each user may use only those computing and information technology resources for which he or she has authorization. Violations include but are not limited to:**

   - using resources without specific authorization
   - using someone else's account and password without their explicit permission or sharing another person's account and password with someone else without their explicit permission
   - accessing files, data or processes without authorization

2. **Computing and information technology resources must be used only for their intended purpose(s). Violations include but are not limited to:**

   - misusing software to hide personal identity, or to interfere with other systems or users

- misrepresenting a user's identity in any electronic communication (e.g. forging an e-mail address)
- using electronic resources for deceiving, harassing or stalking other individuals
- sending threats, "hoax" messages, chain letters, or phishing
- intercepting, monitoring, or retrieving without authorization any network communication
- using university computing or network resources for advertising or other commercial purposes
- circumventing or attempting to circumvent security mechanisms
- using privileged access to university systems and resources for other than official duties directly related to job responsibilities
- making university systems and resources available to those not affiliated with the university
- using former system and access privileges after association with Rutgers has ended

3. **The access to and integrity of computing and information technology resources must be protected. Violations include but are not limited to:**

   - creating or propagating computer viruses, worms, Trojan Horses, or any other malicious code
   - preventing others from accessing an authorized service
   - developing or using programs that may cause problems or disrupt services for other users
   - degrading or attempting to degrade performance or deny service
   - corrupting or misusing information
   - altering or destroying information without authorization

4. **Applicable laws and university policies must be followed including but not limited to respecting the copyrights and intellectual property rights of others. Violations include but are not limited to:**

   - making more copies of licensed software than the license allows
   - downloading, using or distributing illegally obtained media (e.g. software, music, movies)
   - operating or participating in pyramid schemes
   - uploading, downloading, distributing or possessing child pornography
   - accessing, storing or transmitting personal information (e.g. social security numbers, drivers license numbers, credit card numbers) without a valid business or academic reason or transmitting such information without using appropriate security protocols (e.g., encryption).

5. Users must respect the privacy and personal rights of others. Violations include but are not limited to:

- o accessing, attempting to access, or copying someone else's electronic mail, data, programs, or other files without authorization

- o divulging sensitive personal data to which users have access concerning faculty, staff, or students without a valid business or academic reason

Although computing and information technology providers throughout the university are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as safeguarding their account and password, taking full advantage of file security mechanisms, backing up critical data and promptly reporting any misuse or violations of this policy.

C. Privacy

The University recognizes that all members of the University community have an expectation of privacy for information in which they have a substantial personal interest. However, this expectation is limited by the University's needs to obey applicable laws, protect the integrity of its resources, and protect the rights of all users and the property and operations of the University. The University reserves the right to examine material stored on or transmitted through its information technology facilities if there is reason to believe that the standards for acceptable use in this policy are being violated, or if there is reason to believe that the law or University policy are being violated, or if required to carry on its necessary operations. For example, information stored on the University's information technology system may be accessed by the University under certain circumstances, including but not limited to:

1. Access by technicians and administrators to electronic records in order to address emergency problems, routine system maintenance, or other uses related to the integrity, security and availability of the University's information technology systems, including but not limited to:

a. Emergency Problem Resolution – Technicians may access technical resources when they have a reasonable belief that a significant system or network degradation may occur.

b. System-generated, Content-neutral Information – Technicians may access and use system-generated logs and other content-neutral data for the purposes of analyzing system and storage utilization, problem troubleshooting, and security administration.

c. Incident Response - The incident response function within the University Information Protection and Security Office (IPS) is responsible for investigating reports of abuse or misuse of university information technology resources. Incident response staff may use system-generated, content-neutral information for the purposes of investigating technology misuse incidents.

d. Network Communications - Security analysts of the University Information Protection and Security Office (IPS) may observe, capture, and analyze network communications. "Network communications" may contain content data and in some cases this content may be viewed to complete analysis.

e. User Request – Technicians may access information technology resources in situations where a user has requested assistance diagnosing and/or solving a technical problem.

2. Information requested pursuant to New Jersey Open Public Records Act which requires disclosure of electronic communication and other data on the University system subject to the exemptions within that Act. Such access is approved through the office of the University Custodian of Records and all reasonable efforts are made to notify the user in question prior to the release of such information.

3. Information required to comply with a valid subpoena, a court order or e-discovery. Such access is approved through the Office of General Counsel.

4. Audits and investigations undertaken by governmental entities or by University auditors including the Department of Internal Audit, or other University units authorized to carry out University policy.

5. The need of the University to carry on its normal operations, e.g., in the case of accessing the electronic records of a deceased, incapacitated or unavailable individual.

D. Technician and System Administrator Responsibilities:

Technician and System Administrators and providers of university computing and information technology resources have the additional responsibility of ensuring the integrity, security, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose. Technicians and Systems Administrators will not override systems protections unless necessary, and will treat the contents of those systems as private information to the extent possible. Any private information viewed in the course of carrying out these duties must be treated in the utmost confidence.

E. Violations:

- Violators are subject to suspension or termination of system privileges and other penalties.
- If a suspected violation involves a student, a judicial referral may be made to the Dean of Students Office of the school or college of the student's enrollment. Incidents reported to the Dean will be handled through the University Code of Student Conduct.
- If a suspected violation involves a staff or faculty member a referral may be made to the individual's supervisor.