Guidelines for Interpretation and Administration of the Acceptable Use Policy for Computing and Information Technology Resources

These guidelines are meant to assist the University community in the interpretation and administration of the Acceptable Use Policy for Computing and Information Technology Resources. They outline the responsibilities each member of the community accepts when using computing and information technology resources. This is put forth as a minimum set of standards for all areas of the University and may be supplemented with unit specific guidelines. However, such additional guidelines must be consistent with this policy and can not supersede this document.

User Responsibilities:

Use of Rutgers University computing and information technology resources is granted based on acceptance of the following specific responsibilities:

- Use only those computing and information technology resources for which you have authorization.
  For example: it is a violation
  - to use resources you have not been specifically authorized to use
  - to use someone else's account and password or share your account and password with someone else
  - to access files, data or processes without authorization
  - to purposely look for or exploit security flaws to gain system or data access
- Use computing and information technology resources only for their intended purpose.
  For example: it is a violation
  - to send forged email
  - to misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with other systems or users
  - to use electronic resources for harassment or stalking other individuals
  - to send bomb threats or "hoax messages"
  - to send chain letters
  - to intercept or monitor any network communications not intended for you
  - to use computing or network resources for advertising or other commercial purposes
  - to attempt to circumvent security mechanisms
  - to use privileged access for other than official duties
  - to use former privileges after graduation, transfer or termination
- Protect the access and integrity of computing and information technology resources.
  For example: it is a violation
  - to release a virus or worm that damages or harms a system or network
  - to prevent others from accessing an authorized service
  - to send email bombs that may cause problems and disrupt service for other users
  - to attempt to deliberately degrade performance or deny service
  - to corrupt or misuse information
  - to alter or destroy information without authorization
- Abide by applicable laws and university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
  For example: it is a violation
  - to make more copies of licensed software than the license allows
  - to download, use or distribute pirated software
  - to operate or participate in pyramid schemes
  - to distribute pornography to minors
  - to upload, download, distribute or possess child pornography
- Respect the privacy and personal rights of others.
  For example: it is a violation
  - to tap a phone line or run a network sniffer without authorization

- to access or attempt to access another individual's password or data without explicit authorization
- to access or copy another user's electronic mail, data, programs, or other files without permission

System Administrator Responsibilities:
System Administrators and providers of University computing and information technology resources have the additional responsibility of ensuring the integrity, confidentiality, 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 and only when required to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

Security Caveat:
Be aware that 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 the policy.

Violations:
Every member of the University community has an obligation to report suspected violations of the above guidelines or of the Acceptable Use Policy for Computing and Information Technology Resources. Reports should be directed to the unit, department, school, or administrative area responsible for the particular system involved.

If a suspected violation involves a student, a judicial referral maybe made to the Dean of Students Office of the 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 will be made to the individual's supervisor.

BACK TO TOP

For questions or comments about this site, contact webmaster@nbcs.rutgers.edu.