Information Services & Technology
Acceptable Use Policy

I. PURPOSE

IS&T's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to UMDNJ's established culture of openness, trust and integrity. IS&T is committed to protecting UMDNJ's employees, partners and the university from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of UMDNJ. These systems are to be used for business purposes in serving the interests of the university, and of our clients and customers in the course of normal operations. Please review University policies for further details.

Effective security is a team effort involving the participation and support of every UMDNJ employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at UMDNJ. These rules are in place to protect the employee, student and UMDNJ. Inappropriate use exposes UMDNJ to risks including virus attacks, compromise of network systems and services, and legal issues.

II. APPLICABILITY

This policy applies to employees, students, contractors, consultants, temporaries, and other workers at UMDNJ, including all personnel affiliated with third parties. This policy applies to all equipment that is connected to the UMDNJ network. This includes but is not limited to equipment that is owned or leased by UMDNJ.

III. ACCOUNTABILITY

Under the President, the Senior Vice Presidents shall ensure compliance with this policy. The Vice President for Information Systems and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

IV. DEFINITIONS

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.

REFERENCES

A.	Access to University Administered Software Systems	00-01-95-10:00
B.	Information Management	00-01-10-30:00
C.	Rights and Responsibilities for the Use of University-Accessed Electronic Information Systems	00-01-10-40:00

D. Patient Confidentiality and Health Information 00-01-40-60:00
E. Family Educational Rights and Privacy Act 00-01-25-05:00

.

V. POLICY

A. General Use and Ownership

1. While UMDNJ's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the university systems remains the property of UMDNJ. Because of the need to protect UMDNJ's network, management cannot guarantee the confidentiality of information stored on any network device belonging to UMDNJ.
2. Individual departments are responsible for creating guidelines concerning proper use of Internet/Intranet/Extranet systems. Each individual department is responsible for filing their guidelines defining proper use with IS&T Network Security Team, for approval. In the absence of such policies, employees should be guided by UMDNJ's policies on business use, and if there is any uncertainty, employees should consult their supervisor or manager. UMDNJ's policy can be located from the Office of Policy and Project Management web page, please see policy entitled *Rights and Responsibilities for the Use of University-Accessed Electronic Information Systems, coding #00-01-10-40:00.*
3. IS&T recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within UMDNJ may monitor equipment, systems and network traffic at any time, per **IS&T's Audit Policy**.
5. UMDNJ reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

B. Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by university confidentiality guidelines, details of which can be found in University policies. Examples of confidential information include but are not limited to: university private, corporate strategies, competitor sensitive, trade secrets, specifications, patient lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly and user level passwords should be changed every three months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, by locking or by logging-off (control-alt-delete for Win2K users) when the host will be unattended. IS&T Security Team will review and approve exceptions for devices in restricted areas.
4. Use encryption of information in compliance with **IS&T's Acceptable Encryption Use policy**.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised.
6. Postings by employees from a UMDNJ email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UMDNJ, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the UMDNJ Internet/Intranet/Extranet, whether owned by the employee or UMDNJ, shall be continually executing approved virus-scanning software with a current virus database.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

C. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of UMDNJ authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UMDNJ-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

D. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UMDNJ.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UMDNJ or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a UMDNJ computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any UMDNJ account, this includes the operation of personal and non-UMDNJ business related activities and websites.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IS&T is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, UMDNJ employees to parties outside UMDNJ.

E. Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within UMDNJ's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by UMDNJ or connected via UMDNJ's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

VI. NON-COMPLIANCE AND SANCTIONS

Any person found to have violated this policy may be subject to denial or removal of access privileges to the University network; disciplinary action under applicable University policies and procedures up to and including termination; civil litigation; and/or civil or criminal prosecution under applicable state and federal statutes.