I.T. ACCEPTABLE USE POLICY

Policy Number:
Owner Department: Information Technology
Effective Date: February 24, 2011
Approved By: President's Council

I. POLICY TITLE

I.T. Acceptable Use Policy

II. POLICY STATEMENT

Computing and communication resources are provided for the use of faculty, staff, currently admitted or enrolled students, and other properly authorized users and are the property of SCNM. They are to be used for the advancement of SCNM's educational, research, service, community outreach, administrative, and business purposes. When a user's affiliation with SCNM ceases, the Information Technology will terminate access to computing and communications resources and accounts. SCNM may, at its discretion, permit the user to have the access to accounts and e-mail forwarded or redirected for a limited period of time. Alumni are granted permanent SCNM.edu email accounts.

Users of SCNM's computing and communications resources are required to comply with this policy, other applicable SCNM policies and state and federal laws. When necessary, enforcement will be consistent with other applicable SCNM administrative policies and procedures.

III. POLICY STATUS

Revised

IV. DEFINITION(S)

Worms: a software program capable of reproducing itself and spreading from one computer to the next over a network

Spam: mass marketed unsolicited email (junk mail).

Virus: software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer; typically delivered through email and often requires user intervention to activate (such as opening a file or web link).

Chain mail: sent via email to mail recipients enticing them with emotionally-based offers and typically requesting the item be forwarded to others

Denial of service attack: an electronic attempt to make a computer resource unavailable to its intended users

Broadcasting: intentionally transmitting packets that will be received (conceptually) by every device on the network.

Computer accounts: An account created to uniquely identify a computer or individual on a network.

Password: a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource.

Scanning of networks: piece of software designed to search a network host for open ports. An act of sending queries to Internet servers (hosts) in order to obtain information about their services and their level of security. An attack which scans computers ports, a place where information goes into and out of a computer, and effectively identifies open doors to a computer that attackers use

Bridges, routers, and hubs: bridges serve as a logical link between networks and filters traffic at a network boundary; routers are physical devices that join multiple wired or wireless networks together; hubs join multiple computers (or other network devices) together to form a single network segment.

V. PURPOSE

This policy defines the boundaries of acceptable use of computing and communication resources, including computers, networks, electronic mail services, electronic information sources, voice mail, telephone services, and other communication resources. In addition, this policy reflects the goal of SCNM to foster academic freedom while respecting the principles of freedom of speech and the privacy rights of students, faculty, employees, and guests.

VI. SCOPE/KEY STAKEHOLDERS

Stakeholders are defined as SCNM computer network users: Staff, Faculty, Students and alumni.

VII. POLICY ITEMS

A. Uses of Computing and Communications Resources
    a. Requirements for Use:
        i. Users must supply their legal name to Information Technology for the creation of unique user ID's.
        ii. Users must comply with all applicable local, state, and federal laws and regulations, and with SCNM policies.
        iii. Users must respect academic freedom and free speech rights.
        iv. Users must be truthful and accurate in personal and computer identification.
        v. Users must respect the rights and privacy of others, including intellectual property, copyright laws, and personal property rights.
        vi. Users must not compromise the integrity of electronic networks, must avoid restricted areas, and must refrain from activities that may damage the network, or transmitted or stored data.
        vii. Users must maintain the security of accounts and are advised to protect and regularly change their account passwords.
    b. Prohibited Uses

   i. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications, are prohibited.
   ii. Use of computer resources for private business or commercial activities, fund-raising or advertising on behalf of non-SCNM organizations is prohibited.
   iii. The unauthorized reselling of SCNM computer resources is prohibited.

c. Unauthorized use of college trademarks or logos and other protected trademarks and logos is prohibited.
d. SCNM home pages may link to commercial Web sites, but any link that generates, or has the potential to generate, revenue to SCNM or to any individual or company, including click trade or banner advertising, must be approved by the VP Advancement/Marketing and the VP of Finance and Administration.
e. Any alteration of addresses, uniform resource locator (URL), or other action that masks the SCNM.edu domain as a host site is prohibited.
f. Unauthorized anonymous and pseudonymous communications are prohibited. All users are required to cooperate with appropriate SCNM personnel or other authorized personnel when investigating the source of anonymous messages.
g. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.
h. Unauthorized acquisition attempts to acquire, and/or use of passwords of others are prohibited.
i. Unauthorized use and attempts to use the computer accounts of others are prohibited.
j. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
k. Unauthorized modification of or deletion of another person's files, account, or news group postings is prohibited.
l. Use of computer resources or electronic information without authorization or beyond one's level of authorization is prohibited.
m. Interception or attempted interception of communications by parties not authorized or intended to receive them is prohibited.
n. Making computing resources available to individuals not affiliated with SCNM without approval of an authorized SCNM official at or above the level of dean or director is prohibited.
o. Intentionally or recklessly compromising the privacy or security of electronic information is prohibited.
p. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited. The unauthorized storing, copying or use of audio files, images, graphics, computer software, data sets, bibliographic records and other protected property is prohibited except as permitted by law.
q. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited. The intentional propagation of computer "worms" and "viruses," the sending of electronic chain mail, denial of service attacks, and inappropriate "broadcasting" of messages to large numbers of individuals or hosts are prohibited.

r. Failure to comply with requests from appropriate SCNM officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy is prohibited.
s. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access is prohibited.
t. Altering or attempting to alter files or systems is prohibited.
u. Unauthorized scanning of networks for security vulnerabilities is prohibited.
v. Attempting to alter computing or networking components (including, but not limited to, bridges, routers, and hubs) without approval or beyond one's level of authorization is prohibited.
w. Wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services unless approved by an authorized network administrator is prohibited.
x. Negligent or intentional conduct leading to disruption of electronic networks or information systems is prohibited.
y. Negligent or intentional conduct leading to the damage of SCNM electronic information, computing/networking equipment, and resources is prohibited.

B. Information Posted to SCNM Computers or Web Pages
    a. Restriction on Use of Web Pages
        i. SCNM web pages are used only for College business and only authorized individuals may modify or post materials to these pages. No other pages may suggest that they are College Web pages. If confusion is possible, pages should contain a disclaimer and links to SCNM sites.
    b. Responsibilities of Individuals Posting Materials
        i. By posting materials and using College computing facilities, the user represents that he or she has created the materials or that he or she has the right to post or use the materials. The storage, posting, or transmission of materials must not violate the rights of any third person in the materials, including copyright, trademark, patent, trade secrets, and any rights of publicity or privacy of any person. The materials posted must not be defamatory, libelous, slanderous, or obscene.
    c. Responsibilities of Individuals Storing Data on Public Network Folders
        i. SCNM's network provides secure storage space for departments, individuals and a non-secure general purpose repository referred to as a Public folder. Individuals storing information in a Public folder acknowledge the information:
            1. Does not contain confidential informational
            2. Does not contain photographic images unrelated to SCNM activities
            3. Will be removed from public folders as soon as the material in no longer relevant or within 12 months of posting.
    d. College Control of Web Pages
        i. The use of the site is at the sole discretion of SCNM. The College does not guarantee that the user will have continued or uninterrupted access to the site. The site may be removed or discontinued at any time at the discretion of SCNM in accordance with SCNM policy, or as needed to maintain the continued operation or integrity of SCNM facilities.
        ii. SCNM makes reasonable efforts to protect the integrity of the network and related services.

iii. SCNM is not responsible for the backup, disaster recovery, or user access to information posted on personal computers or Web pages.
iv. Access to services and file storage may be approved for emeriti, retired staff, alumni, and guests.

e. The Social Media Policy dictates standards for the use of and posting to social media sites.

C. Electronic Mail and Electronic Communications
   a. Conditions for Restriction of Access to Electronic Mail
      i. Access to SCNM e-mail is a privilege that may be wholly or partially restricted without prior notice and without consent of the user:
         1. if required by applicable law or policy.
         2. if a reasonable suspicion exists that there has been or may be a violation of law, regulation, or policy.
            Or
         3. if required to protect the integrity or operation of the e-mail system or computing resources or when the resources are required for more critical tasks as determined by appropriate management authority.
      ii. Access to the e-mail system requires approval of the appropriate SCNM supervisory or management authority (e.g., department head, system administrator, etc.).
   b. Conditions for Permitting Inspection, Monitoring, or Disclosure
      i. SCNM may permit the inspection, monitoring, or disclosure of e-mail, computer files, and network transmissions when:
         1. required or permitted by law, including public records law, or by subpoena or court order
         2. SCNM or its designated agent reasonably believes that a violation of law or policy has occurred
            Or
         3. Necessary to monitor and preserve the functioning and integrity of the e-mail system or related computer systems or facilities.
      ii. All computer users agree to cooperate and comply with SCNM requests for access to and copies of e-mail messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.
   c. SCNM Responsibility to Inform of Unauthorized Access or Disclosure
      i. If SCNM believes unauthorized access to or disclosure of information has occurred or will occur, SCNM will make reasonable efforts to inform the affected computer account holder, except when notification is impractical or when notification would be detrimental to an investigation of a violation of law or policy.
   d. Prohibition against Activities Placing Strain on Facilities
      i. Activities that may strain the e-mail or network facilities more than can be reasonably expected are in violation of this policy. These activities include, but are not limited to: sending chain letters; "spam," or the widespread dissemination of unsolicited e-mail; and "letter bombs" to resend the same e-mail repeatedly to one or more recipients. In addition the use of streaming radio or video services not directly related to educational mission of the college is prohibited.

e. Confidentiality
    i. Confidentiality of e-mail and other network transmissions cannot be assured. Therefore all users should exercise caution when sending personal, financial, confidential, or sensitive information by e-mail or over the network.
    ii. Personal information stored on College computers is neither protected nor considered private under this policy.

D. Privacy and Security
    a. Routine Logging and Monitoring
        i. Certain central service and network activities from workstations connected to the network are routinely logged and monitored. These activities include:
            1. use of passwords and accounts accessed
            2. time and duration of email activity
            3. volume of data storage and transfers
               and
            4. server space used for e-mail.
    b. Detailed Session Logging
        i. In cases of suspected violations of SCNM policies, especially unauthorized access to computing systems, the IT Director may authorize detailed session logging. This may involve a complete keystroke log of an entire session. In addition, the IT Director may authorize limited searching of user files to gather evidence on a suspected violation.
    c. Responsibility for Data Security
        i. Software and physical limitations, computer viruses, and third party intrusions can compromise security of data storage and communications. SCNM takes reasonable precautions to minimize risk. Information Technology performs regular system backups. It is the user's responsibility to protect their critical data. Individual users and departments should develop policies and practices to ensure that all critical data is stored on a user's network drive or in a departmental network share drive.
    d. Restriction of Access to Sensitive Data
        i. Network policy requires users to change their network password at predefined intervals. This policy also requires network users to implement passwords as defined in the I.T. Password Security Policy.
        ii. All SCNM departments should implement policies to ensure that access to sensitive data is restricted to those employees who have a need to access the information. Passwords restricting access to data system information should be changed on a regular basis and procedures should be developed and implemented to assure password records are regularly updated by appropriate supervisors.
    e. Right to Examine Computers and Equipment
        i. College-owned computers and equipment may be examined to detect illegal software and to evaluate the security of the network.

E. Violations and Enforcement
    a. Reporting Violations

i. Any actual or suspected violation of the rules listed above should be brought to the system administrator of the equipment or facility most directly involved. In the case of a serious violation, a report may be made to Information Technology or the College Legal Counsel.

b. SCNM Response to a Reported Violation
   i. Upon receiving notice of a violation, SCNM may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings.
   ii. A person accused of a violation will be notified of the charge and have an opportunity to respond before SCNM imposes a permanent sanction. Appropriate cases will be referred to the SCNM disciplinary authority appropriate to the violator's status (e.g., Dean of Students or employee's supervisor) or to appropriate law enforcement authorities.
   iii. In addition to sanctions available under applicable law and SCNM policies, SCNM may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, SCNM-administered computing rooms, and other services or facilities.
   iv. If SCNM believes it necessary to preserve the integrity of facilities, user services, or data, it may temporarily suspend any account, whether or not the account user is suspected of any violation. SCNM will provide appropriate notice to the account user. Computers that threaten the security of college systems will be removed from the network and allowed to reconnect only with the approval of network administration.

F. Applicable Law and Policies
   a. SCNM students and employees are bound by all applicable law and college policies.

VIII. RESPONSIBILITY FOR IMPLEMENTATION

IT Director; Network Administrator

IX. APPROVAL BODY

President's Council

X. DATE POLICY APPROVED

February 23, 2011

XI. RELATED POLICIES

IT Password Security Policy

XII. RELATED DOCUMENTS

Form: IT New Hire Checklist
Form: HR New Hire Computer Use

XIII. DATE EFFECTIVE

February 24, 2011

XIV. NEXT REVIEW DATE

As needed

XV. VERSION CONTROL AND CHANGE HISTORY

Version Control	Approved By/Date	Date Effective	Amendment
1	President's Council/ February 23, 2011	February 24, 2011	
2			

XVI. POLICY AUTHOR/CONTACT

Stan Zalewski/Director IT