COMPUTER POLICY:

1. ENGINEERING AND FACILITIES COMPUTER POLICY:

   A. Computers are provided throughout Engineering and Facilities and to be used for MUSC business. The intent in providing this equipment is to support the mission of MUSC, not for personal use.

   B. Individual passwords are used to protect the equipment and the information on the systems, just as locks and keys are used on office and shop doors and on desks and file cabinets.

   C. A supervisor has access to locked offices, desks, file cabinets and lockers used by employees under his supervision. A supervisor (in that line of authority) is also authorized to access an employee’s computer equipment if there is a need for this action. It is recommended that personal information not be stored on MUSC computer equipment. Any personal documents or information stored on MUSC computer systems may be accessed by supervisors, computer support personnel and others should the need arise. As stated earlier, the intent on being assigned the use of MUSC computer equipment is not for personal use; but for MUSC business. Personal documents and information should be maintained at a place other than MUSC.

   D. Personal software is not to be loaded on MUSC computer equipment. This is to prevent unnecessary risk of virus damage to the individual computer, as well as to the entire system.

   E. The MUSC Computer Use Policy is included as part of this policy. Employees who have access to MUSC computer equipment and systems are directed to read and comply with this policy. Among the topics covered by the MUSC Computer Use Policy are privacy, property rights, responsibilities of users, security, copyright and licensing responsibilities, MUSC disciplinary action and prosecution by local, state or federal authorities.

   F. Productivity can be affected when employees use the computer for personal “surfing the Internet” or sending/receiving personal e-mail messages, jokes, and other information. Harassment can occur in the viewing of pornography or other offensive material. If in doubt regarding sending a non-MUSC document, don’t send it. Abusive behavior will not be tolerated and may subject an employee to disciplinary action up to and including termination.

   Employees may occasionally use their computer for a personal e-mail, just as policy allows for an occasional local telephone call, but this is with the understanding that there is right of privacy in these communications or Internet activities. MUSC reserves the right to monitor computer usage without prior notice. Should this cause you concern, it is then recommended that all of your personal computer communications be done on other than MUSC equipment. As previously stated, the intent of providing this equipment is to support the mission of MUSC, and not for personal use.
2. ENGINEERING AND FACILITIES E-MAIL POLICY

E-mail is made available to Engineering and Facilities employees to assist in communication and the efficient completion of daily tasks. However, the informal and relatively unsecured nature of e-mail can cause many problems that might not be obvious to users. This policy will serve to protect other users and the Division by informing users of expected standards of conduct with or received by Engineering and Facilities employees when using the e-mail system. This policy applies to all MUSC Engineering and Facilities employees. Engineering and Facilities reserve the right to change this policy at any time as may be required under the circumstances.

While reviewing the policy, bear in mind that the e-mail system is the property of MUSC and that any employee who violates that policy or uses the electronic mail system for improper purposes shall be subject to discipline, up to and including discharge.

- The electronic mail system hardware is property of MUSC. Additionally, all messages composed, sent or received on electronic mail system are and remain the property of the MUSC. They are not the private property of any employee.
- The use of e-mail system is for the conduct of Engineering and Facilities/MUSC business. Personal usage should be kept to a minimum.
- The e-mail system may not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
- The e-mail system is not be used to create any offensive or disruptive messages. Among those, which are considered offensive, are any messages that contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone’s age, sexual orientation, religious or political believes, national origin, or disability.
- The e-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.
- Engineering and Facilities/MUSC reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of e-mail obtained for legitimate business purposes may be disclosed within Engineering and Facilities without the permission of the employee.

- Engineering and Facilities/MUSC reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of e-mail obtained for legitimate business purposes may be disclosed within Engineering and Facilities without the permission of the employee.
- The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. All passwords must be disclosed to Engineering and Facilities or they are invalid and cannot be used.
• Outside Engineering and Facilities / MUSC’s right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior approval from the MUSC Chief Facilities Officer.

• Employees shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Employees should not attempt to gain access to another employee’s messages without the latter’s permission. All computer codes must be provided to supervisors. No pass code may be used that is unknown to Engineering and Facilities management.

• Sending e-mail from another user’s address for malicious reasons is strictly forbidden. Forgery or attempted forger of e-mail or posting to newsgroups under another user’s address is strictly prohibited. Each user should take measures to ensure that when away from their desk, they do not leave their computer accessible by an unauthorized user.

The user of e-mail is very beneficial in the workplace. However, it should not replace face-to-face or verbal communication in all situations. Please utilize good judgment as to when e-mail is the appropriate means of communication.

3. MUSC COMPUTER USE POLICY:

This policy was unanimously approved by the MUSC Board of Trustees on August 9, 1996.

A. INTRODUCTION

The policy statements which follow serve primarily to aid in the interpretation of, and in a few cases to augment, the University’s general policies on the appropriate use of University Engineering and Facilities, and the University’s general ethics policies for faculty, students, and staff. At a minimum, faculty should refer to the Faculty Handbook, students to the MUSC Bulletin, and staff to the Medical University of South Carolina Human Resources Management Policy Manual for Non-Faculty Personnel (“The Personnel Manual”). The University’s Intellectual Property Policy, which applies to faculty, students, and staff, may be found in the Faculty Handbook.

B. PRIVACY

In general, information stored on computers and the content of electronic communications are considered confidential, unless the owner or sender intentionally makes that information available to other groups or individuals. In particular, personal files on the University’s computers (for example, files stored in a user’s home directory, or on a personal computer) should be considered private to the same degree as personal files in University-assigned space in an office, lab, or desk area. Private communications via computer (for example,
through electronic mail) have the same privacy protection as private
communications via telephone.

Nonetheless, one should exercise caution when committing sensitive information
to storage or transmission on any electronic media, because the confidentiality of
electronic media cannot be guaranteed. Routine maintenance can result in the
contents of files and messages being seen by system or network administrators;
however, network and system administrators are expected to treat the contents
of electronic files and communications as private and confidential. Any
inspection of electronic files or messages, and any action based upon such
inspection, will be governed by all applicable US and SC laws and by University
policies. Note that under the Freedom if Information Act, the files of University
employees (paper or electronic) may be considered public documents, and may
be subject to inspection under the FOIA, through formal University-administered
procedures. The content of electronic files and communications may also be
subject to subpoena in other legal proceedings.

C. PROPERTY RIGHTS

The ownership of the contents of electronic files and messages is a function of
applicable US laws, State laws, and University and departmental policies. University contracts with third parties (for example, software license contracts
and research and sponsored program contracts) may also apply.

The University’s Intellectual Property Policy (see the Faculty Handbook) applies
to all Inventions and Copyrightable Works produced by employees and trainees,
including such works as may be embodied in electronic files.

D. ACADEMIC FREEDOM

Freedom to teach and freedom to learn are inseparable facets of academic
freedom. The freedom to learn depends upon appropriate opportunities and
conditions not only in the classroom, but also on the campus as a whole. The
responsibility to secure and to respect general conditions conducive to the
freedom to learn is shared by all members of the academic community – faculty,
staff, and students. System and network administrators are expected to respect
the University’s academic freedom policies.

No file stored on a University computer system should be removed by a system
administrator without the file owner’s permission unless the file’s presence
interferes with the operation of the system.

No posting to a University-sponsored electronic forum should be removed by a
system administrator unless it violates US law, State law or University policy.

The following principles apply to a University-supported electronic forums which
support the free exchange of ideas among faculty and students (for example,
Usenet news and Internet mailing lists):
1. The same standards of intellectual and academic freedom developed for faculty and student publication in traditional media apply to publication on electronic forums. Note that there are electronic forums and other materials on the Internet and elsewhere that some members of the University community may find offensive. The University cannot restrict the availability of such material, but the display of offensive material in any publicly accessible area, including but not limited to publicly accessible computer screens and printers, may violate other University policies on unacceptable behavior (for example, harassment or discrimination). Similarly, any use of the University computing or network Engineering and Facilities to post offensive materials to electronic forums on the Internet and elsewhere may violate these University policies.

2. The authors of all postings submitted to electronic forums for distribution outside the University should include a disclaimer stating that the opinions expressed therein are not necessarily those of the University.

E. RESPONSIBILITIES OF USERS

All faculty, staff, and students who use University-supported computer and network systems share in the responsibility for upholding the rights of their fellow users. Meeting this responsibility requires adherence to certain rules, outlined below, which apply to all University systems.

1. Appropriate and reasonable use

   a. Computer and network access account should be used only for authorized purposes. Personal use of University computing and network resources is restricted by State law. Section 8-13-700(A) of the South Carolina Ethics Code reads as follows:

      No public official, public member, or public employee may knowingly use his official office, membership or employment to obtain an economic interest for himself, a member of his immediate family, an individual with whom he is associated, or a business with which he is associated. This prohibition does not extend to the incidental use of public materials, personnel, or equipment, subject to or available for a public official's public members, or public employee's use which does not result in additional public expense.

   b. Users should refrain from interfering with other users (for example, consuming gratuitously large amounts of limited system resources such as disk space, CPU time, or printer supplies.)
2. Privacy and Confidentiality
   a. Accessing another user’s files without permission is prohibited.
   b. Accessing any information on a University information system without authorization is prohibited.
   c. Disruption or unauthorized monitoring or interception of electronic communications is prohibited.
   d. Use of any patient or other human subject’s information for any research-related activity without Institutional Review Board (IRB) approval is prohibited.

   These prohibitions apply even in circumstances where the files, information, or messages are not adequately protected against unauthorized access. Any user who discovers a possible "security hole" on an MUSC system is obliged to report it to the system administrator.

3. Security
   a. The users of all systems must maintain adequate passwords on their accounts. Passwords must be kept in strictest confidence, and may not be shared with others without the permission of the system administrator. If a user must temporarily share his or her password with a trusted system administrator (for example, to troubleshoot a problem), then the user should change the password as soon as possible afterwards. Note that passwords should never be shared with [anyone claiming to be] a system administrator without positive identification.
   
   b. The users of all systems must comply with a system administrator's request to change passwords. Whenever possible users should choose their own passwords.
   
   c. The users of all systems are responsible for understanding the system’s default levels of protection applied to files and messages, and for supplementing that protection if necessary for sensitive information.
   
   d. All Engineering and Facilities for incoming remote access to computer systems and communication servers which are directly or indirectly connected to the University’s campus-wide data communications network must provide adequate protection of other networked systems against unauthorized access. [Excerpt from the MUSC Remote Access Security Policy, the full text of which, including a detailed explanation of approved methods for operating dial-up modems, is available from the Center for Computing and Information Technology (CCIT).]
4. Copyright and Intellectual Property
   a. Copyrighted material and software must be used with respect for
      the legal rights of its copyright holder(s).
   b. It is the user’s responsibility to recognize, attribute, and honor
      the intellectual property present on or accessible through
      University computer and communication systems.

5. Licensed (Commercial) Software
   a. The user is responsible for understanding and adhering to the
      licensing terms for all terms for all licensed software which he or
      she knowingly uses.
   b. The making of unauthorized copies of licensed software, even
      when the software is not protected against copying is prohibited.

In addition to the above general rules, there are more specific rules which apply
to many individual University systems. It is the user’s responsibility to ascertain
and follow these system-specific rules. For example, all MUSC patient care
systems have very specific rules protecting the confidentiality of patient
information, and external wide-area networks which you can access through
MUSC’s campus network often have somewhat restrictive “appropriate use”
policies.

F. SANCTIONS

Violations of the MUSC Computer Use Policy by faculty, students, and staff are
 treated as violations of the applicable University ethics policies. Specific
 procedures for dealing with infractions (for example, disciplinary action and
 appeals processes) are detailed in the Faculty Handbook, the MUSC Bulletin,
 and the Personnel Manual.

Violations of public law which involve University computer and communication
 systems may be subject to prosecution by local, state or federal authorities.

University faculty, students, or staff who knowingly violate copyright and/or
 license terms (for example, by making or using an unauthorized copy of a
 copyrighted or licensed software product) may be personally liable for their
 actions.
COMPUTER POLICY

Next Review Date: 7-1-2016

Approved By: Greg Weigle
Chief Facilities Officer
Engineering & Facilities

Effective Date: January 1, 2006

Director of Human Resources
Human Resources