UMCES Computer Use Guidelines
Updated May 2015

The computer departments at each laboratory of UMCES provide individual computer service, open computing facilities, and access to a rich set of software, Internet, and electronics services, including: electronic mail, file transfer and file storage, local networking services, phone service, specialized electronics service and means to create websites on the World Wide Web. UMCES computer accounts are necessary for accessing the UMCES open computing classrooms and file/email access.

Violation of these guidelines constitutes unacceptable use of computing resources, and may violate other University policies and/or state and federal law. Suspected or known violations should be reported to the appropriate UMCES Laboratory IT Director or System Administrator. Violations may result in revocation of computing resource privileges, disciplinary or legal action.

Unacceptable Use - The following types of activities are examples of behavior that are unethical and unacceptable, and in some cases may violate state or federal law:

1. **Unauthorized Access**. Altering system software or hardware configurations without authorization, or disrupting or interfering with the delivery or administration of computer resources.

2. **Software Piracy**. Installing, copying, distributing or using software in violation of copyright and/or software agreements and applicable state and federal laws.

3. **Commercial Use**. Using computing resources for commercial or profit-making purposes without written authorization from the University.

4. **Illegal Activities**. Criminal and illegal use may include obscenity, child pornography, threats, harassment, copyright infringement, defamation, theft, and unauthorized access.

5. **Internet Usage**. University computers and IT resources are not intended for other than professional activities. In addition, peer-to-peer file sharing using programs like NAPSTER, SCOUR and others is discouraged as these put a serious load on the network and can limit availability for legitimate users.

6. **Giving Others Access**. UMCES accounts are provided to students, faculty, staff, and authorized guests for their sole use. Your account is not intended for use by others, including roommates, significant others, or family members. Choose a password that someone cannot readily guess and change it frequently. Your local IT staff can provide guidance on password selection. You are responsible for everything that goes on within your account.

7. **Misrepresentation of Identity**. Attempting to access or accessing another's account, private files, or e-mail without the owner's permission; or misrepresenting oneself as another individual in electronic communication. You are expected to be honest in your electronic communications. Forgery of mail headers or other attempts to make a communication look like it came from someone other than yourself is considered a misuse of your UMCES account.

8. **Mass Mail**. UMCES controlled mail distribution lists and reflectors are for the use of UMCES-affiliated personnel only and should not be released to outside agencies. Also, use of large distribution lists should be limited to essential, work-related mailings only, and not used as a vehicle for an individual to promote his/her personal or political opinions. If mass mailings are warranted, do not attach large files (10MB or larger) to these messages as these attachments are copied to each recipient on the list and can quickly overwhelm the mail system.

9. **Chain Mail**. Mail that demands, via its content or nature, to be re-sent to others is considered chain mail. A user who receives chain mail should delete it. Chain mail is insidious as it grows exponentially, uses system resources for delivery, and utilizes additional system resources as it occupies space in mailboxes. Pyramid schemes that utilize the U.S. postal system for delivery are also illegal.

10. **Spamming Newsgroups**. Spamming includes the act of posting the same or very similar articles to many different news groups. The user should be aware of USENET newsgroup etiquette and pick the most appropriate groups for the particular news item.

Academic Freedom on the Internet - Web pages for faculty, staff, and students at UMCES are an important source of information and communication. Two types of web pages may exist:

- Officially sanctioned pages that are the responsibility of UMCES to maintain and support.

- Individual pages (non-sanctioned) whose content is modified or composed independent of officially sanctioned pages. The main purpose of individual pages will ordinarily be for faculty, students and staff to provide information to colleagues and to the public on topics of research, education, and service.

The same authorship guidelines that apply to all UMCES publications should apply to official and individual pages. This means that principles of academic freedom shall be observed and authors, not the institution, shall take responsibility for the content of their web pages. The following guidelines should be followed regarding UMCES hosted Web pages:

1. UMCES-sanctioned web pages will have a standardized format and will show the UMCES logo. These pages may provide links to non-sanctioned pages where they exist.

2. On all officially sanctioned pages, administrative or supervisory personnel at UMCES shall have editorial control over content.

3. On non-sanctioned pages, authorship shall be identified. Faculty have the responsibility to ensure that non-sanctioned pages under their control are not in violation of law, but faculty also have the further responsibility to ensure that material on web pages is reasonably connected with UMCES duties or with their activities in research, education, and service.

4. The concepts of collegial interactions apply and censorship through denial of access or editorial control over content may occur by a majority vote of the faculty at any one of the three laboratories. We anticipate that this would be an extreme and unlikely (not routine) event.

5. It is the right of Administrators to require, if necessary, that non-sanctioned web pages omit the UMCES logo and post a disclaimer stating that the material does not indicate an official UMCES endorsement.

6. It is the normal policy of UMCES that academic freedom should apply. To this end, disciplinary action should normally not be taken toward faculty members regarding the content of non-sanctioned web pages, unless (a) such content violates law or rules of conduct as described under other provisions, and (b) such other laws or provisions are *not* at odds with the premise of academic freedom.

Computer Security – The following items are institutional best practices to be followed by all UMCES

1. Daily backup of document files on local machine pertinent to UMCES and network shares.
2. Installation of current anti-virus software provided by UMCES IT.
   a. Clear communication that users are required to ensure that their anti-virus signature is updated or current, and
   b. Periodic independent review of users' computers to ensure that their AV solution is updated with the latest signatures. The results of this review should be documented.

3. Create strong passwords where possible and do not share them with anyone forany reason. A strong password has at least eight characters, uses a combination of numbers, upper and lowercase letters, and uses at least one special character (such as !@#$%^&*).
4. Log off, lock your screen, or use a password-activated screensaver whenstepping away from your computer for more than 15 minutes. Workstations will be set to auto lock after 15 minutes ofinactivity.
5. Avoid opening e-mail embedded web links and attachment if you cannot verify the source.
6. Do not store personally identifiable information such as social security number, income tax records, credit card numbers, and banking information on your workplace computer or network shares.

Administration - The maintenance, operation, and security of computing resources require responsible University personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the Maryland Access to Public Records Act, other applicable state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations.

Questions regarding the UMCES Computer Use Guidelines should be directed to UMCES Director of IT who can be reached at kflorez@umces.edu or (410) 221-2021.

Questions regarding your UMCES account should be directed to your local IT staff.