I. Overview

This document constitutes a campus-wide policy intended to allow for the proper use of all UACCB computing and network resources, effective protection of individual users, equitable access and proper management of those resources. This document should be broadly interpreted. This policy applies to UACCB network usage even in situations where it would not apply to the computer(s) in use. This policy applies to all those who use UACCB computers. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to computing and networking services.

All members of the UACCB community are encouraged to use electronic communications for college-related activities and to facilitate the efficient exchange of useful information. However, access to college electronic communications services is a privilege, and certain responsibilities accompany that privilege. People who use UACCB communications services (such as email) are expected to use them in an ethical and responsible manner, following general guidelines based on common sense, common decency, and civility applied to the networked computing environment.

Access to the UACCB network is a privilege, not a right. Access to networks and computer systems owned or operated by UACCB requires certain user responsibilities and obligations and is subject to campus policies and local, state, and federal laws. Appropriate use should always be legal and ethical. Users should reflect academic honesty, mirror community standards, and show consideration and restraint in the consumption of shared resources. Users should also demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and annoyance. Appropriate use of computing and networking resources includes instruction; independent study; authorized research; independent research; communications; and recognized student and campus organizations, and agencies of the college. UACCB computing and networking resources may not be used for commercial or profit making purpose, for political purposes, or for personal benefit where such use incurs a cost to the College and is not academically related.

II. Practice

Users of UACCB's information technology resources are expected to abide by the following policies:

1. Information technology resource usage is restricted to faculty, staff, and students currently enrolled in UACCB credit and non-credit classes, and authorized public.

2. Network users will be allowed access to other networks and computers external to UACCB. Because each network or system has its own set of policies and procedures, users must abide by the policies and procedures of networks/systems both internal and external to UACCB.

3. UACCB is not responsible for information either transmitted or received by users of its computer network/system.

4. The content and maintenance of a user's electronic mailbox is the user's responsibility. As such, the user must take the following responsible action:
   a. Check electronic mail on a regular basis and delete unwanted messages immediately.
   b. Never assume that electronic mail messages are private; others may be able to read or access a user's mail. UACCB computer user may assume in general, electronic communications transmitted across a network should never be considered private or confidential. When considering the safety and security of a communication, it is best to think of email and instant messages like postcards—viewable by anyone with access.
   c. Electronic communications should meet the same standards for distribution or display as if they were tangible documents or instruments. Identify yourself clearly and accurately in all electronic

communications. Concealing or misrepresenting your name or affiliation to dissociate yourself from responsibility for your actions is never excusable.

5. The content and maintenance of a user's storage area is the user's responsibility. As such, the user must take the following responsible action:
   a. Keep the number of files to a minimum.
   b. Routinely and frequently check for viruses.
   c. Make sure that data is stored on the local computers is copied to a specified network location so that information is backed up.

6. Users are **NOT AUTHORIZED TO:**
   a. **Copy, rename, alter, examine or delete** the files or programs of another employee or a UACCB department without written permission. All files and programs are legal property of UACCB.
   b. Use a computer to **interfere with individual and/or institutional rights,** including but not limited to the following
      i. Sending of **abusive** or **otherwise objectionable messages** to others;
      ii. **Sending of messages** that are likely to result in the loss of recipient's work or systems;
      iii. Any type of use that would **cause congestion of the networks** or otherwise interfere with the work of others;
      iv. Use the computer resources **for personal activities** not related to the mission of UACCB;
      v. Posting of **public service events not approved** by the appropriate Vice Chancellor.
   c. **Create, disseminate, or run a self-replicating program ("virus"),** whether destructive in nature or not.
   d. Use computers maintained by UACCB for **non-college projects** without the approval of the appropriate Vice Chancellor.
   e. **Tamper with switch settings, move, reconfigure,** or do anything that could damage files, terminals, computers, printers, or other equipment.
   f. **Collect, read, or destroy output** other than their own work without permission unless the account is designated for group work.
   g. Use the **computer account of another person without permission** unless the account is designated for group work.
   h. **Copy any copyrighted software.** Users should be aware that it is a criminal offense to copy any software that is protected by copyright.
   i. Use licensed software in a manner inconsistent with the licensing agreement.
   j. Surf, view, or download any **sexually explicit media** in the computer labs. Sexually explicit media shall not be displayed on any UACCB terminals, microcomputers, printers, or any other equipment.
   k. Access or attempt to **access a host computer,** either at UACCB or through a network, without the owner's permission.
   l. Use **log-in information** belonging to another person
   m. Use UACCB equipment for the purpose of **playing non-instructional games.**
   n. Indiscriminately **engage in talk sessions** with on-or off-campus sites.

7. Harassment
   No user, under any circumstances, should use UACCB's computers or networks to harass any other person. The following constitutes computer harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such

communication to cease (such as debt collection); (4) Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; and (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or to threaten invasion of the privacy of another.

8. Privacy
   Users of UACCB's computing and technology resources do not have a legal expectation of privacy. However, UACCB respects the contents of users' files and monitors the network in accordance with network monitoring standards. UACCB does not review electronic communication for the purpose of determining whether impermissible activity is occurring. In the course of assuring the viability of the UACCB network, IT administrators may become aware of activity that poses a risk to the network's proper operation. In such cases, IT administrators may need to disable or block access to the services or systems involved if they are deemed to pose a risk to the network's optimal performance.
   UACCB does not monitor personal Web pages for the purpose of determining content. However, when credible evidence of illegal or otherwise impermissible activity is reported, appropriate action will be taken.

9. System administration access
   A system administrator (i.e., the person responsible for the technical operations of a particular machine) may access others' files for the maintenance of networks and computer and storage systems, such as to create backup copies of media. System administrators may become aware of file content while dealing with specific operational problems. Usage logs are frequently kept to diagnose such problems. UACCB will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance includes providing, when required, copies of system files, email content, or other information ordered by the court.

10. Monitoring of usage, inspection of files
    Users should also be aware that their use of UACCB computing resources is not completely private. While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for maintaining network availability and performance.
    The College may also specifically monitor the activity and accounts of individual users of the Institute's computing resources, including individual login sessions and communications, without notice. This monitoring may occur in the following instances:
    - The user has voluntarily made these activities accessible to the public.
    - It reasonably appears necessary to do so to protect the integrity, security, or functionality of the College or to protect the College from liability.
    - There is reasonable cause to believe that the user has violated, or is violating, this policy.
    - An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
    - Upon receipt of a legally served directive of appropriate law enforcement agencies.
    - Upon receipt of an FOI request as governed by state law.

    Any such individual monitoring, other than that specified in "(1)", required by law, or necessary to respond to bona fide emergency situations, must be authorized in advance. The appropriate unit head will be informed as time and the situation will allow.

11. Suspension of individual privileges
    UACCB Information Services may suspend computer and network privileges of an individual for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well-being of other members of the campus community or college property. Access will be promptly restored when safety and well being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of the Vice Chancellor for Enrollment

Management and Student Services (for students) or the employee's department in consultation with the Office of Human Resources (for employees).

Process for suspension of students' individual privileges:
Anyone who breaches the policies and procedures of the UACCB computer usage policy will be subject to the following action (disciplinary action may also be taken through the Student Conduct Process):
First offense: Individual is served a warning letter.
Second offense: Individual is served a second warning letter, and computer usage is suspended for one week.
Third offense: Individual is served a third and final warning letter and his or her account will be disabled for the remainder of the semester.

Additional possible consequences of a student's failure to comply with this policy are covered in the Student Conduct section of the Handbook. An employee's failure to comply may be sanctioned by UACCB. At the supervisor's discretion, a range of sanctions from verbal warnings to termination may be applied. User actions in violation of state or federal law may be prosecuted.

12. No food or drinks are allowed in computer laboratories.

13. UACCB reserves the right to close laboratories or curtail use of computing facilities if the above policies and/or procedures are violated.

III. Clarifying Points

1. Civil discourse is at the heart of a higher education community free of intimidation and harassment. It is based upon a respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable and essential, bear in mind that it is your responsibility to do so in a way that advances the cause of learning and mutual understanding.

Adopted: October 9, 2009