# Table of Contents

Overview ......................................................................................................................................................... 3

I.  General Use.................................................................................................................................................. 4

II.  Responsible/ Appropriate Use of Facilities .............................................................................................. 5

   A.  System Accounts...................................................................................................................................... 5

   B.  Computing Access..................................................................................................................................... 5

   C.  Internet Usage.......................................................................................................................................... 6

   D.  Intellectual Property................................................................................................................................. 6

   E.  Network Activities.................................................................................................................................. 6

   F.  Email and Electronic Communication Activities.................................................................................... 7

III. Security and Proprietary Information......................................................................................................... 9

IV.  Unacceptable Use..................................................................................................................................... 10

   A.  General Lab Rules................................................................................................................................... 10

   B.  System Accounts..................................................................................................................................... 11

   C.  Computing/ Networking Equipment Access.......................................................................................... 11

   D.  Email and Electronic Communication Activities................................................................................... 13

   E.  Network Activities.................................................................................................................................. 14

   G.  Internet Usage......................................................................................................................................... 15

   F.  Intellectual Property................................................................................................................................. 16

V.  Enforcement............................................................................................................................................. 17
Overview

This Acceptable Use Policy governs the use of all Information Technology resources provided by School of Accounting and Management to accomplish the mission and goals of the University. Information Technology resources may be used for lawful and permitted purposes only.

This policy applies to Information Technology and systems inside the University utilized by students, staff, faculty and any other persons representing or acting on behalf of the college or accessed for the purpose of utilizing the resources.

In support of its mission of teaching, research, and public service, and within its institutional priorities and financial capabilities, School of Accounting and management provides access to computing, network and information systems and services for the students

Information Technology systems include Internet access, computer equipment, software, operating systems, networking devices, storage media, network accounts and electronic mail.

Issues concerning improper use of the Information Technology resources should be brought to the attention of the IT Helpdesk. It is the responsibility of every user to know these guidelines and to conduct their activity accordingly. The use of these systems is a privilege and all users are expected to act responsibly and to follow the University’s guidelines, policies, procedures and laws.
I. General Use

The School of Accounting and Management defines and provides access to institutional computers, information systems and networks. Reliable and safe access to the University's information resources requires that users accept their responsibilities to behave in ways that protect the community, and by so doing, they also preserve their own access.

All users must respect the rights of others, the integrity of the facilities and controls which are implemented to maximize the community's reliable access, and all pertinent license and contractual agreements that underlie the University's technology infrastructure. It is the policy of the University to deny access to any member of the user community who violates this policy or who uses the University’s technology resources to violate other duly established policies or laws.
II. Responsible/ Appropriate Use of Facilities

All users have the responsibility to operate School of Accounting and Management’s computing systems in an ethical, lawful and responsible manner. The following are intended to illustrate the range of unacceptable actions rather than to exhaustively elaborate all specific behaviors that may violate the principle.

A. System Accounts

Users must adamantly protect their personal passwords

Passwords are the basic security mechanism which authenticates individuals as eligible to use University resources. The username and password also authorizes individuals to perform specific actions based on the identity of the user. Many legal and ethical violations begin when the culprit obtains use of someone else’s password, wittingly or unwittingly shared.

Passwords should be chosen that are difficult to guess and should not be written down. Under no circumstances should a password be shared with a family member, friend or acquaintance, much less any stranger or caller.

Users should immediately report any suspected unauthorized use of their username to their system administrator.

Users must respect the privacy of others’ passwords, information and communication, and may not attempt to use University resources to gain unauthorized access to any site or network or to maliciously compromise the performance of internal or external systems or networks.

B. Computing Access

The School of Accounting and Management does not permit the modification of Lab workstations or the software that is installed. The workstation is provided for the purpose of doing work for the University. If there is a requirement for special configurations or special software, the request must first be made to the IT Department.
C. Internet Usage

All students are expected to use the Internet responsibly and productively. Internet access is provided for to facilitate studies and research.

All Internet data that is composed, transmitted and/or received by the organization’s computer systems is considered to belong to School of Accounting and Management.

The equipment, services and technology used to access the Internet are the property of the School of Account and Management and the organization reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.

All sites and downloads may be monitored and/or blocked by School of Accounting and Management if they are deemed to be harmful or malicious to business.

D. Intellectual Property

Intellectual property is the backbone of a university, and all members of the university community should respect the work of others inside and outside the academy. Users must observe all laws relating to copyright, trademark, export and intellectual property rights.

E. Network Activities

Academic integrity dictates that members of the University community be accountable for their actions.

The University administers its technology resources on a shared-use basis for the benefit of the entire community. This is only possible when all members of the community respect the need of others for services.

The School of Accounting and Management is committed to be a good institutional citizen of the Internet, noting that non-cooperating institutions are sometimes blacklisted from certain services which could prevent members of the University community from achieving their legitimate academic requirements.
As a general rule, the University tries to be permissive rather than prohibitive in these matters, but certain behaviors by individuals can compromise the availability and reliability of services for the entire community.

Examples of such activities include the unauthorized running of "server" programs on institutional systems.

While it attempts to manage resources on a content-neutral basis, the University does reserve the right to curtail specific uses of its technology infrastructure that unduly interfere with the institution’s ability to provide the best possible service to the overall community.

F. Email and Electronic Communication Activities

Users must ensure that their electronic communications do not infringe the rights of others and are conducted in accord with the same standards of behavior that apply in other forms of communication

The privilege of Internet access offers numerous opportunities to interact with others all over the world. As an institution of higher education the University supports open and unrestricted communication by members of its community. However, many people have a tendency to send email, post messages, or engage in other behaviors that they would never think to perform in person. Electronic communication may lack the visual and verbal cues such as a smile or tone of voice that indicate when someone is joking, so misinterpretation may be more likely than in-person. For this reason, it is suggested that people exercise even more care in their on-line communication than face-to-face.

The same legal and policy standards that define intimidation, harassment or invasion of privacy apply to the electronic environment. For example, persistence in sending unwanted email constitutes harassment and is unacceptable if not illegal.

Finally, users should be aware that each specific on-line forum or mailing list might have specific standards of content and behavior to which its members are expected to adhere. These may range from "no anonymous messages" to "no posting of job ads on this mailing list." The University will cooperate in helping the managers of external forums enforce their standards, just as we expect other institutions to cooperate in helping members of the SAM community manage their forums based on the public standards of behavior established for their group.
University resources are intended to be used for institutional purposes and may not be used for private gain.

The University provides information technology resources at great expense for the purpose of supporting its mission (learning, teaching and research). It is expected that usage will be primarily educational in nature in support of this mission.

All applicable laws and policies relating to the ethical use of public resources apply to University information technologies as well.
III. Security and Proprietary Information

- Users are responsible to keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

- All PCs, laptops and workstations should be secured with a password-protected by locking their workstation when the computer will be unattended.

- The school is not responsible for any files lost due to virus scans.

- Each user is responsible for checking any software he/she introduces to any computer or the college network for computer viruses. If a user introduces a virus because he/she did not follow standard checking procedures, the school is not responsible for any files lost due to virus scans performed by the lab machines.

- Students should use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

- They should also exercise caution when receiving work from other students who could have possible virus infections.

- The School of Accounting and Management is not responsible for any infections contracted by the student due to their computer use.
IV. Unacceptable Use

Under no circumstances is any individual authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing School of Accounting and Management - owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

A. General Lab Rules

All Information Technology resources and computer equipment are the property of the college. It is the user’s responsibility to learn the proper use and care of all equipment.

Theft, failure to observe copyright laws, or tampering with computers or networks will place violators in jeopardy of prosecution through law enforcement and University agencies.

- Lab consultants are provided to assist the users with questions and to help with hardware and software problems, but are not there for the assistance of students with their course work or any personal matters
- Packages/containers of food or drinks is not allowed in labs or around any IT Infrastructure.
- Sound levels in the lab must be kept to a minimum.
- Groups are allowed in computer labs but cannot disrupt the learning environment for others, and if they do so will be asked to disband.
- No disruptive behavior is allowed in the labs.
- Cell phones must be taken out of the lab when a call is made or answered.
- Stations left unattended for more than 10 minutes may be reassigned to another user.
- Moving around of the lab equipment and/or cables is strictly prohibited.
- The labs are for University students, staff and faculty ONLY. We reserve the right to check IDs.
B. System Accounts

Distributing or making your password or another person’s password to available to unauthorized persons or otherwise attempting to evade, disable or “crack” password(s) or other security provisions or assisting others in doing so threatens the work, privacy and well-being of others and is prohibited.

This includes family and other household members when work is being done at home.

C. Computing/ Networking Equipment Access

All Information Technology resources and computer equipment are the property of the School of Accounting and Management. It is the student’s responsibility to learn the proper use and care of all equipment.

Failure to observe copyright laws, or tampering with computers or networks will place violators in jeopardy of prosecution through law enforcement and University agencies.

- Users must not store or run programs intended to obtain others’ passwords. Users must not look over others’ shoulders to try to obtain passwords or otherwise try to obtain unauthorized access to the information or communication of others.

- It is a breach of this policy for any individual to disable or interfere with the functioning of any virus or security software loaded on any equipment unless they have clearance from IT staff.

- Users may not attempt to gain unauthorized access to other systems, networks and services external to the University via the University’s Internet or other network connections. Nor may programs be stored or executed that attempt to gain unauthorized system-level access to computers or network devices either inside or external to the University.

- Users may not store or execute programs or engage in or abet any activities designed to test or compromise system or network performance without the prior written authorization of the responsible system administrator(s). This includes programs that introduce a virus, worm or other destructive/disruptive programs. Users may not launch "denial-of-service" attacks against internal or external systems and networks from within the University.
• Using the computers for display of sexually explicit images or sound obscene email is extremely prohibited.

• Under no circumstances will excuses be accepted that such behaviors were intended purely for educational purposes or to help system administrators improve security.

• Relocation of any hardware is only to be done with the prior approval of the IT Manager.

• Individuals are responsible to ensure that all issued must be kept secure at all times to prevent damage.

• The Equipment should at no point in time be close to food or liquids.

• Any damage to computers or any equipment should be reported to the IT Department without delay. The same applies to any apparent malfunction of equipment.

• Using the computers for display of sexually explicit images or obscene content is extremely prohibited.

• No individual should intentionally and without authorization, access, modify, damage, destroy, copy, disclose, print, or take possession of all or part of any computer, computer system, networking device, network, software, data file, program, database, or any other College IT resource. This includes:
  o Gaining access by willfully exceeding the limits of authorization
  o Attempting (even if unsuccessful) to gain unauthorized access through fraudulent means
  o Gaining access by using another person’s name, password, access codes, or personal identification
  o Attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes
D. Email and Electronic Communication Activities

A School of Accounting and Management computing asset should not be used to actively engage in procuring or transmitting material that is in violation of laws.

It is prohibited to make fraudulent offers of products, items, or services originating from any School of Accounting and Management account.

Laws relating to child pornography, obscenity and defamation apply in electronic environments and the University will willingly cooperate in the prosecution of individuals formally charged with such offenses.

Users may not engage in the transmission of unsolicited bulk email ("spamming"), regardless of how important it may seem to the sender. This policy shall in no way limit the use of email as a legitimate means for the University community to share information and communication.

School of Accounting and Management prohibits use of University resources for private business purposes and under no circumstances may individuals use institutional technology resources for commercial purposes without prior written authorization.

This includes activities such as hosting a commercial home page, or providing friends who are not members of the University community with access to institutional equipment and services. Users may not run private servers or bulletin board systems for non-University purposes through University networks or provide such connectivity to others. Political campaigning may not be engaged in using the University's electronic information systems.

Users may not initiate or participate in the targeting of a particular person or system with mass quantities of email ("mail bombs").

Activities such as spam, chain letters, and mail bombs degrade performance of networks and systems, may violate agreements with third parties such as the University's Internet Service Providers.

Violations may be cause for the revocation of the offender's access to University resources.
E. Network Activities

Individuals utilizing the School of Account and Management prohibited from performing any of the following activities:

- Connecting of one’s own equipment to the wired LAN without authorization from the IT Manager is strictly prohibited.

- Introduction of malicious programs into the network or server. For example: viruses, worms, Trojan horses, e-mail bombs, etc.

- Sniffing networks or undertaking comparable measures to obtain access to passwords or other information not made publicly available by the owner.

- Engaging in activities which compromise institutional systems or network performance for others.

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorized to access. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinger floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited.

- Executing any form of network monitoring which will intercept data not intended for the students’ use.

- Circumventing user authentication or security of any computer, network or account.

- Falsely representing oneself or “spoofing” another physical network connection. Academic integrity dictates that members of the University community be accountable for their actions. Users may not attempt to represent their network activities as originating from a network address other than the actual source (i.e. "spoofing").
G. Internet Usage

Individuals utilizing the Internet provided by the School of Account and Management are prohibited from performing any of the following activities:

- Sending or posting confidential, political, obscene, discriminatory, harassing, or threatening messages or images on the Internet using the IT infrastructure.

- Downloading text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.

- Using computers to perpetrate any form of fraud, and/or software piracy.

- Downloading, copying or pirating software, film or music and electronic files that are copyrighted or without authorization.

- Stealing, using, or disclosing someone else’s password without authorization.

- Sharing confidential material, trade secrets, or proprietary information outside of the University.

- Hacking into unauthorized websites.

- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.

- Introducing malicious software onto the school network and/or jeopardizing the security of the organization’s systems.

- Passing off personal views as representing those of the organization.

If any student is unsure about what is constituted as acceptable Internet usage, then he/she should get in contact with the IT Helpdesk for further guidance and clarification.
F. Intellectual Property

Intellectual property is the backbone of a university, and all members of the university community should respect the work of others inside and outside the academy.

Software may not be duplicated or installed except in strict accordance with applicable licensing agreements.

University servers and networks are not to be used to house or distribute unauthorized software, music, video or other information resources.

The University will actively participate in the prosecution of members of the community who violate the law, for example, by mounting illegal music or software distribution servers using University resources.

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 School of Account and Management.

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 School of Accounting and Management or the end user does not have an active license is strictly prohibited.
V. Enforcement

School of Accounting and Management is authorized by University regulations to enforce these policies and regulations.

Such enforcement may include temporary or permanent reduction or elimination of access privileges with prior notification and approval by the Administration, except in extraordinary cases in which any delay may seriously threaten the integrity of facilities, user services or data.

In such extraordinary cases, when the University believes it necessary to preserve the integrity of facilities, user services, or data, they may, with prior notice and approval of the Administration, suspend any account, whether or not the account owner (the user) is suspected of any violation.

Non-compliance with any of the provisions of this policy may subject the user to disciplinary action, sanctions or criminal prosecution, as well as personal liability in a civil suit.

Any actual or suspected violation of the policies within this document must be brought to the attention of the IT Manager, other appropriate IT personnel, and/or other University authorities.