SUMMARY:

I. It is the mission of Information Technology Services (ITS) at Coastal Carolina University to provide emerging, reliable and cost-effective technology resources and services to enhance student learning and improve teaching as well as to augment the research and administrative functions of the University. Coastal Carolina University maintains policies for the use and security of its information technology resources to ensure that all use of Coastal Carolina University’s information technology resources support the University’s mission as a public comprehensive liberal arts institution.

II. ITS is responsible for securing the University's network and computing systems in a reasonable and economically feasible manner against unauthorized access and/or abuse, while making information technology resources accessible for authorized and legitimate users. Information technology resources are defined as computer systems, networks, and data and information resources including software, data, files and all associated content regardless of the form or the location, as well as computers, devices and telephones. These policies apply to all electronic records of the University, regardless of their form or location. All users of University information technology resources are required to adhere to these policies.

POLICY:

I. GENERAL COMPUTING POLICY

   A. All computer systems that are the property of Coastal Carolina University and/or the State of South Carolina should be used only for University-related business.

   B. Any unauthorized, deliberate action that violates posted policy, damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is prohibited regardless of system location or time duration.
C. Only software approved/relevant to the user’s University-related duties should be installed on a computer system. A list of ITS-supported/approved software is available on the ITS website.

D. The copying or sharing of copyrighted materials, software, video and audio files (including MPEG files) without the express written permission of the owner or the proper licensing authority is prohibited.

E. Due to the increased risk of electronically transmitted viruses, it is suggested that software upgrades, installation files and other executable files (.exe files) should only be downloaded and installed from the Internet after consultation with ITS staff.

F. Students must have antivirus software on their computers and must update their antivirus program definitions regularly. ITS provides an antivirus application for students at no additional cost.

G. Unless advised otherwise, students must update their operating system regularly to ensure system integrity and security.

H. The use of University technology resources (e.g., computers, computer systems, facilities and/or services) for commercial purposes is prohibited.

I. The installation of University wired and/or wireless routers, bridges and similar equipment without the expressed consent of ITS is prohibited.

II. NETWORK ACCOUNTS AND SECURITY

A. Once a user receives an ID to access network and computer systems, the user is responsible for all actions taken while using that ID. Because users of the network may be allowed to access other networks (and/or the computer systems attached to those networks):
   1. Applying for a user ID under false pretenses is prohibited.
   2. Sharing user credentials with any other person is prohibited. If someone else uses your user credentials, you will be responsible for the actions that other person performed. Sharing of user credentials may result in the loss of all University computer accounts.
   3. Using your computer as a server on the network (or any directory or file on your computer) is prohibited unless access is password protected. Any files considered public should be copied to an appropriate directory that is accessible from the network.
   4. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
   5. Attempts to evade or change resource quotas are prohibited.
6. Continued impedance of other users through mass consumption of system resources/bandwidth, after receipt of a request to cease such activity, is prohibited.
7. Use of systems and/or networks to gain unauthorized access to remote systems is prohibited.
8. Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote/local system, is prohibited.
9. Use of systems and/or networks to copy or share copyrighted materials, software, audio and video files (including MPEG files) is prohibited.
10. Decryption of system or user passwords is prohibited.
11. The copying and/or modification of system files is prohibited.
12. Any intentional attempt to "crash" network systems or programs is prohibited.
13. Any attempt to secure a higher level of privilege on network systems is prohibited.
14. The willful introduction of computer "viruses" or other disruptive or destructive programs into University or external networks is prohibited.
15. Any attempt to intercept and/or monitor network traffic is prohibited.

III. ELECTRONIC MAIL (EMAIL)

A. The use of email on the University network system is contingent upon the following:
1. The email system is University property and should be used only for University-related purposes.
2. The University reserves the right to monitor email and Internet usage. (For students and parents, please refer to the Family Educational Rights and Privacy Act (FERPA).
3. There are no privacy rights in the creation, sending or receipt of email.
4. In response to system restrictions and space limitations, pictures, graphics, movies or any other email file attachments in the system without a valid business reason should be kept to a minimum.
5. Whenever electronic mail is sent, the sender’s name and user ID are included in each message. The sender is responsible for all electronic mail originating from their user ID. Therefore:
   a. Forgery (or attempted forgery) of email messages is prohibited.
   b. Attempts to read, delete, copy or modify the email of other users are prohibited.
   c. Attempts to send harassing, obscene or threatening email to another user are prohibited.
   d. Attempts to send junk mail, "for-profit" or chain email are prohibited.

IV. WIRELESS TECHNOLOGY
A. ITS is responsible for managing the technology infrastructure of the Coastal Carolina University Data Network, including wireless network access.
   1. Wireless access points (WAPs) intended for colleges, departments or divisions of the University must be approved and registered in ITS prior to installation. Unapproved WAPs will not be allowed to connect to the campus network.
   2. The installation of non-University wireless access points (WAPs), routers, bridges and similar equipment without prior consent from ITS is prohibited.

V. NEW AND EMERGING TECHNOLOGIES

New and emerging technologies are to be approved in advance by the appropriate departmental official, the University Technology Council (if applicable) and ITS prior to installation or use on University resources. To ensure data integrity/security, efficiency, effectiveness, compatibility with University systems, the non-redundancy of system resources and the strategic alignment of the University mission, while also meeting the technology needs of the University, technology adoption should follow the appropriate channels and the IT Governance structure.

VI. SOCIAL MEDIA

All University social media properties should have a specific purpose and topics should be relevant to the mission of Coastal Carolina University. As such, each Social Media Administrator must be familiar with and agree to comply with the following guidelines and must adhere to the University Social Media Policy:

A. A social media account in the name of a recognized Coastal Carolina University entity may be established and/or maintained only by those authorized to represent that department, division, college and/or organization.

B. All social media accounts representing Coastal Carolina University are to be registered through the Office of University Communication.

C. Every University account is to include in its description that it is the official presence of the respective department, division, college and/or organization. For example, “Welcome to the official Facebook page for the Office of University Communication at Coastal Carolina University.”

D. All University social media accounts are to be linked to a University email address for the department or the account administrator, not to a private, personal account, where applicable.

E. More than one University employee must have administrative access to the social media account to post items and keep the account current and correct. All comments are to be moderated and refreshed in a timely manner consistent with the
social media outlet. In the event that a site requires an individual account, a unique account should be created expressly for this purpose. Administrative access to the account will be relinquished at graduation, termination, voluntary cessation of employment, or assignment to another job.

F. Comments that are obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful or embarrassing to another person or any other person or entity are not to be posted. Confidential or proprietary information about Coastal Carolina University, its students, faculty, staff and affiliates may not be posted or solicited. All laws and Coastal Carolina University policies apply, including, but not limited to: FERPA (Family Educational Rights and Privacy Act), HIPAA (Health Insurance Portability and Accountability Act), and the state’s Freedom of Information Act (SCFOIA).

G. External comments from the community on University social media accounts do not imply endorsement of that content by Coastal Carolina University. Posts on a personal social media account that identify the author as a member of the Coastal Carolina University community should clarify that the views are those of the individual and not those of the University.

H. Coastal Carolina University is a public institution. As such, commercial promotion on University social media accounts is prohibited (for example, a discount at an area restaurant or business). If a business posts an advertisement or solicitation on a University social media property, it will be deleted.

I. In compliance with state ethics guidelines and state law, the Coastal Carolina University name or marks are not be used to promote or endorse any cause or political party or candidate.

VII. HARDWARE SANITATION

The South Carolina Division of Technology Operations mandates that all equipment (e.g., computers, copy machines and electronic media) that may contain intellectual property or personal information must be sanitized prior to transfer for other uses or for disposal. Departments should consult with ITS prior to disposing of any computer equipment.

VIII. VIOLATIONS OF THIS POLICY

A. Users of the University network and systems are responsible for respecting and adhering to local, state, federal and international laws. Users who violate any such laws may be subject to prosecution and/or litigation. The University will fully comply with any complainants to provide any information necessary for prosecution and/or litigation. Activities on the University network may be recorded and may be turned over to the appropriate legal authority.
B. Deliberate attempts to violate the provisions of this policy may result in immediate disciplinary action, regardless of the success or failure of the attempts. The disciplinary action may include permanent loss of all computer accounts, suspension (for students), dismissal (for employees), and/or legal prosecution. Disciplinary action may be administered by University Police (consistent with University policies) and/or the FBI.