Section 11.0 Information Technology

Introduction

Section 11.0, Information Technology, covers all aspects of EGSC technology including the general policies and procedures, information security and usage policies.

Table of Contents

11.1 Campus Computer and Network Usage Policy
11.2 Support Services Policy
11.3 Wireless Network Access Policy
11.4 Acceptable Use Policy
11.5 IT Equipment Acquisition/Asset Management and Confirmation Policy & Procedure
11.6 Computer Anti-Virus Policy
11.7 IT Incident Response Policy & Procedure
11.8 Remote Network Access Policies
11.9 Approved Software/Applications Policy
11.10 Campus Email Policy
11.11 Institutional Website Policy
11.12 Telephone Use by Faculty/Staff
11.13 Computer Lab/Workstation Usage Policy
11.1 Campus Computer and Network Usage Policy

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community." - The EDUCOM Code.

1. BACKGROUND AND PURPOSE

This document constitutes a College-wide policy intended to allow for the proper use of all East Georgia State College computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This should be taken in the broadest possible sense. This policy applies to East Georgia State College network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to these services.

Academic Divisions may add, with the approval of the Division Chairperson, individual guidelines which supplement, but do not relax, this policy. In such cases, the Division should inform their users and Information Technology prior to implementation.

Access to networks and computer systems owned or operated by East Georgia State College imposes certain responsibilities and obligations and is granted subject to College policies and local, state, and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use of computing and networking resources includes instruction; independent study; independent research; communications; and official work of the offices, departments, recognized student and campus organizations, and agencies of the College.

2. DEFINITIONS

2.1. Authorized use
Authorized use of East Georgia State College-owned or operated computing and network resources is use consistent with the education, and service mission of the College, and consistent with this policy.

2.2. Authorized users
Authorized users are: (1) current faculty, staff, and students of the College; (2) anyone connecting to a public information service (see section 6.5); (3) others whose access furthers the mission of the College and whose usage does not interfere with other users' access to resources.
In addition, a user must be specifically authorized to use a particular computing or network resource by the campus department responsible for operating the resource.

3. INDIVIDUAL PRIVILEGES

It is the following individual privileges, all of which are currently existent at East Georgia State College, that empower each of us to be productive members of the campus community. It must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities.

3.1. Privacy
To the greatest extent possible in a public setting we want to preserve the individual's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that East Georgia State College computer systems and networks are public and subject to the Georgia Open Records Act. Users, thus, utilize such systems at their own risk.

3.2. Freedom of expression
The constitutional right to freedom of speech applies to all members of the campus no matter the medium used.

3.3. Ownership of intellectual works
People creating intellectual works using East Georgia State College computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Properties (Board of Regents Policy Manual, section 6.3 and any subsequent revisions), and related East Georgia State College policies.

3.4. Freedom from harassment and undesired information
All members of the campus have the right not to be harassed by computer or network usage by others. (See section 4.1.3.)

4. INDIVIDUAL RESPONSIBILITIES

Just as certain privileges are given to each member of the campus community, each of us is held accountable for our actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across campus engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom are grounded on each person's developing the skills necessary to be an active and contributing member of the community. These skills include an awareness and knowledge about information and the technology used to process, store, and transmit it.

4.1. Common courtesy and respect for rights of others
You are responsible to all other members of the campus community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.
4.1.1. Privacy of information
Files of personal information, including programs, no matter on what medium they are stored or transmitted, may be subject to the Georgia Open Records Act if stored on East Georgia State College's computers. That fact notwithstanding, no one should look at, copy, alter, or destroy anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so.

Similarly, no one should connect to a host on the network without advance permission in some form. People and organizations link computers to the network for numerous different reasons, and many consider unwelcome connects to be attempts to invade their privacy or compromise their security.

4.1.2. Intellectual property
You are responsible for recognizing (attributing) and honoring the intellectual property rights of others.

4.1.3. Harassment
No member of the community may, under any circumstances, use East Georgia State College's computers or networks to libel, slander, or harass any other person.

The following shall constitute Computer Harassment:
   a. 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
   b. Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease
   c. 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)
   d. Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another
   e. Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

4.2. Responsible use of resources
You are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources or from using them in whatever ways have been proscribed by the College and the laws of the State and Federal governments. Details regarding available resources are available in many ways, including consulting with the Information Technology Department at East Georgia State College, conferring with other users,
examining on-line and printed references maintained by Information Technology and others, and visiting the Student Computer Labs.

4.3. Game playing
College computing and network services are not to be used for recreational game playing. East Georgia State College reserves the right to block access to recreational game-playing web sites that may be accessed by any or all personal computers, laptops, servers, or similar computerized equipment attached to the East Georgia State College data network.

4.4. Information integrity
It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that you compile or use. Do not depend on information or communications to be correct when they appear contrary to your expectations; verify it with the person who you believe originated the message or data.

4.5. Use of desktop systems
You are responsible in coordination with Information Technology for the security and integrity of College information stored on your personal desktop system. This responsibility includes making regular disk backups, controlling physical and network access to the machine, and installing and using virus protection software. Avoid storing passwords or other information that can be used to gain access to other campus computing resources.

4.6. Access to facilities and information
The "Rules for Use of East Georgia State College Computer Laboratories" should be followed regarding the general use of all College Computer Labs and the equipment contained in each lab. These rules are posted in each computer laboratory and are accessible on the College web page.

4.6.1. Sharing of access
Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.

4.6.2. Permitting unauthorized access
You may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 2.2.)

4.6.3. Use of privileged access
Special access to information or other special computing privileges are to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as private.

4.6.4. Termination of network / account access
When a student, faculty or staff member (including instructors and participants of continuing education courses or other guests of East Georgia State College requiring network access / email accounts) is no longer an active member of East Georgia State College, the individual's network /
email account access will be terminated accordingly. The following list includes but is not limited to categories and situations that warrant the termination of an EGSC network / email account:

Students: Students who have graduated from EGSC; students in non-attendance for one or more academic years. This information will be obtained and monitored via the BANNER student system.

Faculty / Staff: Termination of employment, resignation, retirement. For staff and faculty whose employment with EGSC is terminated, the respective network / email account will be terminated the same date as the employment termination date. In order for the necessary network / email account termination process to take place on the day of termination, the college's Office of Human Resources will inform the Vice President for Information Technology concerning faculty and staff employment terminations.

Guests of EGSC requiring temporary network / email account access:
Temporary guest network / email account access will be terminated immediately upon the completion / conclusion of event(s) where an EGSC guest network / email account access was required.

For all categories, (students, faculty / staff, CE Instructors & participants, and guest users) immediate termination of network / email account access will occur in the event an individual uses an EGSC network / email account in an unauthorized manner. The sections (4.7 through 4.12) listed below include but are not limited to types of activities that could be deemed as unauthorized use of an EGSC network / email account and could lead to termination of network / email account access.

4.7. Attempts to circumvent security
Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by system administration personnel.

4.7.1. Decoding access control information
You are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

4.7.2. Denial of service
Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any College computer system or network are prohibited.

4.7.3. Harmful activities
The following harmful activities are prohibited:
   a. creating or propagating viruses
   b. disrupting services
   c. damaging files
   d. intentional destruction of or damage to equipment, software, or data belonging to East Georgia State College or other users, and the like
4.7.3.1. File sharing and P2P activities
File sharing and peer-to-peer (P2P) activities are not allowed on the East Georgia State College data network.

4.7.4. Unauthorized access
You may not:
   a. damage computer systems, obtain extra resources not authorized to you, deprive another user of authorized resources, gain unauthorized access to systems, by using knowledge of:
   b. a special password, loopholes in computer security systems, another user's password, access abilities you used during a previous position at the College

4.7.5. Unauthorized monitoring
You may not use computing resources for unauthorized monitoring of electronic communications.

4.8. Academic dishonesty
You should always use computing resources in accordance with the high ethical standards of the College community. Academic dishonesty (plagiarism, cheating) is a violation of those standards.

4.9. Use of copyrighted information and materials
You are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other material, in violation of copyright.

4.10. Use of licensed software
No software may be installed, copied, or used on College resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

4.11. Political campaigning; commercial advertising
Board of Regents policy (section 9.6.1) states "The use of USG materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden." The use of College computers and networks shall conform to these policies.

4.12. Personal business
Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to East Georgia State College, except:
   in connection with scholarly pursuits (such as faculty publishing activities); or in a purely incidental way. This and any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to
resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive. State law restricts the use of State facilities for personal gain or benefit.

5. EAST GEORGIA STATE COLLEGE PRIVILEGES
Our society depends on institutions like East Georgia State College to educate our citizens and advance the development of knowledge. However, in order to survive, East Georgia State College must attract and responsibly manage financial and human resources. Therefore, East Georgia State College has been granted by the State, and the various other institutions with which it deals, certain privileges regarding the information necessary to accomplish its goals and to the equipment and physical assets used in its mission.

5.1. Allocation of resources
East Georgia State College may allocate technology resources in differential ways in order to achieve its overall mission.

5.2. Control of access to information
East Georgia State College may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with the laws of Georgia and the United States and the policies of the College and the Board of Regents.

5.3. Imposition of sanctions
East Georgia State College may impose sanctions and punishments on anyone who violates the policies of the College regarding computer and network usage.

5.4. 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. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

5.5. Monitoring of usage, inspection of files
Departments of East Georgia State College operating computers and networks may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, etc. These units may review this data for evidence of violation of law or policy, and other purposes. When necessary, these units may monitor all the activities of and inspect the files of specific users on their computers and networks. Any person who believes such monitoring or inspecting is necessary must obtain the concurrence of the Office of the Vice President for Student Affairs and Information Technology. In all cases all individuals' privileges and right of privacy are to be preserved to the greatest extent possible.

5.6. Suspension of individual privileges
Departments of East Georgia State College operating computers and networks 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 President for Student Affairs (for students) or the employee's department in consultation with the Vice President for Fiscal Affairs (for employees).

6. EAST GEORGIA STATE COLLEGE RESPONSIBILITIES

6.1. Security procedures
East Georgia State College has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged.

6.2. Anti-harassment procedures
East Georgia State College has the responsibility to develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks and to impose appropriate penalties when such harassment takes place.

6.3. Upholding of copyrights and license provisions
East Georgia State College has the responsibility to uphold all copyrights, laws governing access and use of information, and rules of organizations supplying information resources to members of the community (e.g., acceptable use policies for use of Internet).

6.4. Individual department responsibilities
Each department has the responsibility of:
   a. enforcing this policy
   b. providing for security in their areas
   c. providing individuals equipped with College-owned desktop systems with resources for regular disk backups (software, hardware, media, and training)

If warranted by the importance and sensitivity of information stored and processed in their facility on College-owned desktop systems, a department also has the responsibility of:
   a. performing and verifying integrity of regular media backups
   b. employing appropriate security-related software and procedures
   c. guarding confidentiality of private information, including user files and system access codes
   d. controlling physical access to equipment
   e. providing proper physical environment for equipment
   f. providing safeguards against fire, flood, theft, etc.
   g. providing proper access administration; e.g., prompt and appropriate adjustment of access permissions upon a user's termination or transfer
   h. controlling and recording software and configuration changes
   i. monitoring any system logs for access control violation attempts

East Georgia State College’s Information Technology Department or appointed representative(s) serves:
as the first point of contact for unit personnel seeking problem resolution, information, and other assistance regarding computing and networking to facilitate interaction between the departments and the Office of Information and Instructional Technology at the Board of Regents.

6.5. Public information services
Department and individuals may not configure computing systems to provide information retrieval services to the public at large. (Current examples include "anonymous ftp", "Web", and "gopher.") However, centralized computing hardware and software is available for delivery of public information services, where particular attention is paid to the following sections of this policy:

2.1 (authorized use [must be consistent with College mission]), 3.3 (ownership of intellectual works), 2.1, 2.2, 4.2 (responsible use of resources), 4.9 (use of copyrighted information and materials), 4.10 (use of licensed software), and 6.4 (individual unit responsibilities). Usage of public services will not cause computer or network loading that impairs other services.

7. PROCEDURES AND SANCTIONS

7.1. Investigative contact
If you are contacted by a representative from an external organization (District Attorney's Office, FBI, GBI, private security firm, etc.) who is conducting an investigation of an alleged violation involving East Georgia State College computing and networking resources, immediately inform the college's Vice President for Information Technology and the College's President and/or Vice President for Academic Affairs. Refer the requesting agency to the College's Vice President for Information Technology who will provide guidance regarding the appropriate actions to be taken.

7.2. Responding to security and abuse incidents
All users and departments have the responsibility to report any discovered unauthorized access attempts or other improper usage of East Georgia State College computers, networks, or other information processing equipment. If you observe, or have reported to you (other than as in 7.1 above), a security or abuse problem with any College computer or network facilities, including violations of this policy:

Take immediate steps as necessary to ensure the safety and well-being of information resources. For example, if warranted, the Information Technology Department should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 5.6).

Ensure that the following departments/people are notified: (1) Vice President for Information Technology, (2) your department head for employees (2) Office of the Vice President for Academic Affairs for students.
Reports of all incidents will be forwarded to Student Affairs (for apparent policy violations by students) or the department head (for employees), and to the Information Technology Department.

7.3. First and minor incident
If a person appears to have violated this policy, and (1) the violation is deemed minor by the Information Technology Department, and (2) the person has not been implicated in prior incidents, then the incident may be dealt with at the Information Technology Department or other department level. The alleged offender will be furnished a copy of the College Computer and Network Usage Policy (this document), and will sign a form agreeing to conform to the policy.

7.4. Subsequent and/or major violations
Reports of subsequent or major violations will be forwarded to Student Affairs (for students) or the department head (for employees) for the determination of sanctions to be imposed. Departments should consult the Office of Vice President for Fiscal Affairs/Personnel Office regarding appropriate action.

7.5. Range of disciplinary sanctions
Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the College, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws; the College will carry out its responsibility to report such violations to the appropriate authorities.

7.6. Appeals
Appeals should be directed through the already-existing procedures established for employees and students of East Georgia State College.

11.2 Support Services Policy

Scope of Policy
Support for the microcomputer systems owned by East Georgia State College is provided by the staff of the college's Information Technology Department. This office should be contacted when information or support is needed concerning college-owned microcomputer systems and software. The staff of the Information Technology Department office are also available for consultation on the purchase of workstations and software. Information Technology staff will secure all quotations for computer equipment purchases. Please refer to the college's IT Equipment Acquisition / Asset Management & Configuration Policy & Procedures document for additional information regarding purchasing IT-related equipment.

Objectives
The staff members of the College's Information Technology Department are not responsible for providing technical support to faculty, staff, students or other related parties for personally owned IT equipment and/or software.
**Note of Exception**

- The only exception to the Information Technology Department's staff being responsible for providing support for personally owned IT equipment (i.e., notebook, laptop computer) is (1) for assisting faculty, staff, students or guests of the college who are experiencing problems accessing the college's wireless Internet service or (2) for providing assistance to faculty & staff for problems utilizing the EGSC VPN remote access.

- To facilitate this support, an East Georgia State College Information Technology Department "Campus Computer Wireless Network Access Assistance Agreement" form must be signed by the user prior to support being provided. A copy of this form is included at the end of this policy.

Faculty / staff and other related parties requiring assistance with any college-owned IT equipment should first complete a work request via the college's online work request system. If a user is unable to complete the request due to the malfunction of his/her computer, the user should ask the division secretary or other staff / faculty person to submit the request. Work order requests include items such as troubleshooting hardware and software; installation and set up of new systems; and installation of new software. Faculty and staff must not install and set up new equipment and software or move existing equipment. These tasks must be completed by Information Technology staff.

Information Technology staff are responsible for the operation and maintenance of the academic computer labs. Only Information Technology staff may perform maintenance tasks on existing equipment, order and set up new equipment, and install/uninstall software. ALL computer systems located in the college's academic labs must have the necessary security software installed. Only the Information Technology staff may install this software. Request for maintenance of new equipment and software should be completed via the college's online work order system. (NOTE: Each semester, faculty will be notified (via email) of a deadline for submitting software installation requests for the next semester. After the deadline has passed, any request for software installation for the following semester must be approved by the Vice President for Information Technology.)

All campus microcomputer systems are initially covered under warranties. After such warranties expire, decisions will be made to either continue the warranty with the vendor or to maintain systems using Information Technology staff. Consultation with Information Technology staff is recommended before a decision is made. Information Technology staff will coordinate repairs with outside vendors. Cost of extended warranties and repairs will be charged to the appropriate division and department budgets.
11.3 Wireless Network Access Policy

Scope of Policy
East Georgia State College utilizes multiple wireless network access points throughout the campus. These access points provide wireless connectivity to the campus network and allow for users' mobility while using the campus network. To help ensure the security of the campus network via wireless access points, the following guidelines must be followed:

Guidelines of Policy
1. All campus wireless access points have authentication and/or encryption enabled.

2. A "Faculty / Staff" wireless network and a "Student / Guest" wireless network have been created. For a user to be able to access the Faculty / Staff wireless network, the user must have an active, valid EGSC domain user account. However, user access via the Student / Guest wireless network is controlled using policies and firewall rules, which prevent Internet / network activities not permitted. The Campus Computer and Network Usage Policy as well as the Acceptable Use Policy lists the acceptable and unacceptable use of the campus network.

3. Any user (faculty, staff, student or other parties) needing to connect a device via wireless network access shall first contact Information Technology in order for the device to be properly configured for accessing the campus network via wireless connection.

4. Only wireless access points that have been purchased by East Georgia State College and configured by the College's Information Technology staff may be connected to the college's data network.

11.4 Acceptable Use

Overview
Internet / Intranet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of East Georgia State College.

Effective security is a team effort involving the participation and support of every East Georgia State College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose
The purpose of this policy is to outline the acceptable use of computer equipment belonging to East Georgia State College. These rules are in place to protect East Georgia State College, its employees, students and other users of the College's information technology. Inappropriate use
exposes East Georgia State College to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope
This policy applies to faculty, staff, students and other users (i.e., participants of East Georgia State College's Life Long Learning programs, campus visitors), contractors, consultants, temporaries, and other workers at East Georgia State College, including all personnel affiliated with third parties. This policy applies to all IT resources owned by or leased by East Georgia State College.

Policy

General Use and Ownership
1. Because of the need to protect the East Georgia State College network and IT resources/equipment, the College's Information Technology department cannot guarantee the confidentiality of information stored on any network or storage media device belonging to East Georgia State College.
2. All users (identified in Section 3.0 of this policy) are responsible for exercising good judgment regarding the reasonableness of personal use.
3. Any information users consider sensitive or vulnerable should be encrypted.
4. For security and network maintenance purposes, East Georgia State College's Information Technology Department has the right to monitor any of its IT equipment/resources, systems and network traffic at any time.
5. East Georgia State College's Information Technology Department staff reserve the right to audit / monitor / scan the college's network and/or systems and devices that connect to the college's network to ensure compliance with this policy.
6. Faculty, staff, students and other parties (e.g., participants in the College's continuing education / Life Long Learning programs) needing to connect personally owned devices to the college's network must obtain prior approval from the College's Information Technology Department.
7. All microcomputer systems connecting to the campus network must have a minimum of 10/100MB Ethernet cards installed to allow for proper connections to the College network.
8. Wiring for the campus network and any future networks installed on campus will be twisted pair category 5e (minimum requirement) cabling within the buildings and multimode fiber optic cable between buildings.
9. Only the College's Information Technology staff is authorized to provide support, perform installations of new equipment, and/or configure devices for the campus network.

Security and Proprietary Information
1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
   a. Users will be required to change their respective passwords at a minimum of 90-day intervals.
2. All PCs, laptops and workstations should be secured with a password-protected Microsoft screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (use the "control-alt-delete" option Windows 2000 and XP users) when the host will be unattended.

3. Because information contained on portable computers as well as public network storage space are especially vulnerable, special care should be exercised in storing documents of a critical nature.

4. Postings by East Georgia State College faculty, staff and students with an East Georgia State College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of East Georgia State College, unless posting is in the course of business duties.

5. All PCs, laptops, PDAs, workstations and related electronic devices used by faculty, staff and students that are connected to the East Georgia State College Internet/Intranet/Extranet, whether owned by faculty, staff or students or by East Georgia State College, shall be continually executing approved virus-scanning software with a current virus database.

6. Faculty, staff and students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

**Unacceptable Use**

The following activities are prohibited.

Under no circumstances is an employee, student or other user of East Georgia State College's information technology infrastructure authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing East Georgia State College-owned information technology resources.

All of the items listed in the sections below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable and/or prohibited use.

**System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. 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 East Georgia State College.

2. Viewing pornographic or other offensive sites

3. Using campus Internet / Peachnet services for accessing / utilizing web-based game sites, including, but not limited to, web sites that include any form of gambling.

4. Engaging in electronic "pranks" such as mail bombing based on victim's sex, etc.

5. 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 East
Georgia State College and/or the user of East Georgia State College's information technology resources does not have an active license is strictly prohibited.

6. Downloading, copying and/or storing of copyrighted video, music files (and similar type files) via any device connected to the East Georgia State College data network

7. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The College's Information Technology Department and/or appropriate management should be consulted prior to export of any material that is in question.

8. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

9. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

10. Using an East Georgia State College IT resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

11. Making fraudulent offers of products, items, or services originating from any East Georgia State College network account. A network account includes accounts used by faculty, staff, students and other users of the college's information technology resources.

12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the East Georgia State College employee, student or other user of the college's information technology infrastructure is not an intended recipient or logging into a server or account that the East Georgia State College employee, student or other user of the College's information technology infrastructure is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

13. Port scanning or security scanning is expressly prohibited.

14. Executing any form of network monitoring which will intercept data not intended for the employee, student or other college information technology user's host, unless this activity is a part of the listed individuals' normal job/duty.

15. Circumventing user authentication or security of any host, network or account.

16. Interfering with or denying service to any user other than the College's user's host (for example, denial of service attack).

17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Peer-to-peer file-sharing software and related activities.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7. Users of the East Georgia State College email system must use their East Georgia State College email accounts only in support of academic pursuits and/or college business.

**Enforcement**

Any East Georgia State College employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Students of East Georgia State College found to have violated this policy may be subject to academic disciplinary action, (including being suspended from East Georgia State College for a period of time to be determined by the College's senior administration.) Other user's (e.g., participants in East Georgia State College's continuing education programs and the like) found to have violated this policy will be asked to withdraw from the specific program(s) with no reimbursement of program fees or monies paid to participate in the program(s).

Depending upon the scope of the incident, all individuals found to be in violation of this policy may be subject to penalization under local, state and/or federal laws and regulations.

**Definitions**

**Term Definition**

*Spam* Unauthorized and/or unsolicited electronic mass mailings.

**11.5 IT Equipment Acquisition/Asset Management and Confirmation Policy & Procedures**

**Scope of Policy**

This policy is to facilitate the purchasing and use of IT / microcomputer equipment and software used on the East Georgia State College campus. This policy is to formalize the procedure for the approval, acquisition, and management of hardware and software for microcomputer systems and other related IT systems throughout the College. All departments / units of the college are covered by this plan.

**Objectives**

The primary goals of this policy are as follows:

1. Formalize the local approval process for the purchase of microcomputer systems.
2. Establish steps for the approval process.
3. Establish standards for hardware and software for microcomputers.
4. Establish standards for communication and networking capabilities for microcomputer systems.
5. Provide detailed information about standards for microcomputer systems in order that appropriate systems meeting standards are easily identified.
Approval Process – Policies and Procedures
The approval process for the purchase of IT equipment and/or microcomputer system hardware and software will consist of the following steps:

1. Prior to purchasing any microcomputer system or related IT equipment, the requestor must first consult with the college's Information Technology Department to ensure that the system / equipment and/or software will function properly with the college's network configuration and other related IT configurations. In addition, by consulting with the Information Technology Department prior to purchase, this helps to ensure no duplication in equipment or services will occur.

2. All requests for purchasing microcomputer systems and related IT information equipment will require the completion of the college's departmental request form or purchase card request form – both of these forms are available via the College's Intranet site – wwi.ega.edu.

3. Prior to submitting request to the College's business office and/or department / division head, all requests must be routed to the College's Vice President for Information Technology for approval. If needed, the request may be returned to the originator for corrections and/or changes. The Vice President for Information Technology will assist the requestor in preparing the request for approval.

4. If a request is not approved by the Vice President for Information Technology, the request will be returned to the originator with comments and an explanation of the disapproval.

5. All purchase requests will adhere to current University System of Georgia purchasing procedures.

Hardware Policies, Procedures, and Standards
The following minimum standards will be followed when requesting computer workstations:

1. Intel Pentium IV, or greater, microprocessor
   HP is currently the state vendor of choice for computer workstations.
   No Apple / Macintosh computers may be ordered unless obtaining prior approval from the Vice President for Information Technology.


3. Monitors – 1024 x 768 VGA non-interlaced for Intel machines. Minimum 17 inch flat panel displays should be obtained.


5. Ethernet card capable of connection to campus network – minimum 10/100/1000MB card.

6. Minimum three-year warranty for parts, service, onsite service.

All microcomputer systems will be purchased from state contracts. All requests must give the name and location of recommended vendor and state contract number. Requests for microcomputers from sources other than state contracts will not be approved unless the equipment requested is not available from a state contract.
Computer systems and peripherals will be installed/moved, maintained, inventoried only by Information Technology staff. The exception will be the college's Plant Operations staff, who often assist the Information Technology Department with moving / relocating IT equipment. Information Technology will maintain an inventory of College computer systems in an Access database. Included in the database is the hardware information of the computer – processor, type, RAM, hard drive, IP address, Mac address, and college decal inventory number (if available). Also included are the employee and division responsible for the equipment. An inventory of software loaded on each computer is maintained to ensure that license agreements are not violated and that users do not download software that could interfere with the supported software already installed.

The staff members of the EGSC Information Technology Department are not responsible for providing technical support to faculty, staff, students or other related parties with personally owned IT equipment and/or software.

- The only exception to the Information Technology Department's staff being responsible for providing support for personally owned IT equipment (i.e., notebook, laptop computer) is (1) for assisting faculty, staff, students or guests of the college who are experiencing problems accessing the college's wireless Internet service or (2) for providing assistance to faculty & staff for problems utilizing the EGSC VPN remote access. Please refer to the "Information Technology Support Services Policy" for additional information regarding this issue.

Life expectancy of microcomputer systems and related information
Microcomputer systems that were purchased by the College will continue to be used / refurbished for a period not to exceed five (5) years. Only staff of the College's Information Technology Department may perform refurbishing tasks. Systems that have become outdated or that have surpassed the five-year life expectancy period will be sent to the local state surplus facility or transferred to other qualifying State of Georgia entities. Under no circumstances may any college-owned computer related equipment (whether outdated or otherwise) and/or software be loaned to (temporarily or long-term) individuals or other parties.

Software Policies, Procedures, and Standards
(Please refer to the East Georgia State College Approved Software/Applications Policy for additional information regarding approved software and applications.)

The following standards will be followed when requesting software:
1. Operating system for workstation machines is Windows 7.
2. The college’s approved office application is Microsoft Office Professional Edition – current version.
3. The college’s approved Virus protection software is McAfee.
4. Only the following Email applications will be supported by Information Technology: Eudora, Outlook, Outlook Express.

- Any software that must be installed on one or more of the college's network servers must first be approved by the College's Information Technology Department. The installation of such software will be done only by Information Technology staff.
- All requests for software will be subject to the review of the Vice President for Information Technology.
- Each semester, faculty will be notified (via email) of a deadline for submitting software installation requests for the next semester. After the deadline has passed, any request for software installation for the following semester must be approved by the Vice President for Information Technology.
- Software requests for the college's academic labs will be reviewed by the division chairperson and approved by the Vice President for Information Technology.
- All software and licenses will be received and inventoried by the Information Technology staff. The software and licenses will be stored in the Information Technology Department. Where economically feasible, software licenses will be purchased for the College through the Information Technology Department.
- All software will be loaded and installed by Information Technology staff.
- Information Technology staff will request quotes from vendors for software and hardware.

11.6 Campus Anti-Virus Policy

Scope of Policy
This focus of this policy is to ensure that all IT-related devices that connect to the East Georgia State College campus data network have antivirus software installed. This is necessary for preventing computer related viruses, worms, etc., from infecting college-owned (and non-college-owned) IT equipment and the college data network.

Regulations of Policy
1. All information technology equipment that is owned by the college and that connects (wired or wireless) to the East Georgia State College data network must have a current version of the campus supported antivirus program installed. The virus definition file must also be current. Information Technology Staff install the anti-virus application on all college-owned IT equipment and this application must not be uninstalled by the user. Please contact Information Technology for assistance with this issue.

2. All information technology equipment that is not owned by the College and that connects (wired or wireless) to the East Georgia State College data network must have a current version (virus definition file must also be current) of an antivirus program installed.

3. Any user (faculty, staff, student or other participant of an East Georgia State College program or activity) who wishes to connect (wired or wireless) a "personally" owned information technology device to the College network should first contact Information Technology to ensure that an antivirus program has been installed on the device and that the program is current with respect to virus definition files. This also applies to current operating system updates / patches.

4. All computer workstations located in public access areas of the college (i.e. library, Cyber Cafe) will have current versions of the antivirus program currently being utilized and supported by the College's Information Technology Department.
5. All computer workstations located in student computer labs and other labs accessible to students and public users will have current versions of the antivirus program currently being utilized and supported by the College's Information Technology department.

6. All computer workstations located in faculty / staff / work student areas will have current versions of the antivirus program currently being utilized and supported by the College's Information Technology Department.

11.7 Information Technology Incident Response Policy & Procedures

I. Introduction
This policy addresses IT incident response issues involving the College's IT resources.

The policies and procedures listed in this document provide a mechanism for East Georgia State College faculty, staff and students to report any potential IT-related security incidents.

II. Definitions
IT Resource: A system or application that consists of computer hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network infrastructure, E-mail and web based services.

Security Incident: An incident meeting one or more of the following conditions:
Any potential violation of Federal law, Georgia law or East Georgia State College Policy or Plan involving an East Georgia State College IT Resource.

A breach, attempted breach or other Unauthorized Access of an East Georgia State College Information Technology Resource. The incident may originate from inside the East Georgia State College network or via an outside entity.

Internet worms, Trojans, viruses and similar destructive files / services

Any action and/or conduct using in whole or in part an East Georgia State College Information Technology Resource which could be construed as harassing, or in violation of any East Georgia State College policy or state / federal regulation.

Unauthorized Access: Any action or attempt to utilize, alter or degrade an IT resource owned or operated by East Georgia State College in a manner inconsistent with the college policies.

III. Reporting and Response Procedures
All incidents involving East Georgia State College's IT resources will be handled via the following procedures:
1. Department or Division Manager will be notified of incident.
2. Department or Division manager will communicate incident to Vice President for Information Technology. If it is unclear as to whether an issue / situation should be considered an IT security incident, the Department or Division manager should contact the Vice President for Information Technology for assistance.

3. The Vice President for Information Technology, Department or Division Manager will communicate incident to college's senior administration. The college's Human Resources Officer, and if necessary, the College's Public Safety Office will also be notified of incident.

4. Depending on scope of incident, the USG’s Office of Information Services (ITS) will also be contacted.

5. If warranted, local law enforcement officials will be notified.

6. All issues (cause, scope, resolution) relating to the security breach incident will be documented by and retained in the offices of the College's senior administration. Any costs associated with the security breach will also be documented.

7. Individuals (faculty, staff or student), who report a breach of security incident will receive appropriate feedback and updates regarding the incident from one or more of the following areas: College's Senior Administration; Human Resources Department; College’s Public Safety Office; department / division manager; Vice President for Information Technology.

8. Individuals reporting a breach of security incident will be assured of confidentiality, and if necessary, appropriate protection.

Additional items regarding Reporting and Response:

With the exception of items listed below, it is imperative that any investigative or corrective action be performed ONLY by a member of East Georgia State College’s Information Technology Department.

1. When faced with a potential IT-related security situation, faculty and staff should do the following:
   - If the incident involves a compromised computer system, do not alter the state of the computer system. The computer system should remain powered on and all currently running computer programs should be left as is. Do not power down the computer or restart the computer.

2. Immediately disconnect the computer / laptop or other IT connected device from the campus network by removing the patch cable from the back of the computer. If the computer, laptop or device is utilizing wireless network connectivity, the system's wireless network hardware should be disabled via the Network Settings in the Control Panel or via the appropriate system configuration tool.

11.8 Remote (Off-campus) Network Access Policy

Scope of Policy
Remote (off-campus) access to IT services at East Georgia State College is provided via a VPN (virtual private network) secured connection. The VPN provides a secure mechanism for EGSC
Guidelines of Policy

1. Faculty and staff wishing to utilize the VPN remote access service must first contact the EGSC Information Technology Department so that necessary account configurations may be made.

2. Faculty and staff utilizing the remote VPN access must not disclose their VPN account credentials with others (including other faculty and staff).

3. Instructions for accessing the EGSC VPN are available on the EGSC intranet website, wwi.ega.edu. For additional information / questions, please contact the EGSC Information Technology department.

4. When utilizing the VPN access, faculty and staff must adhere to the East Georgia State College Campus Computer and Network Usage Policy and Acceptable Use Policy.

5. Faculty and staff should refer to the East Georgia State College Information Technology Support Services Policy for additional information regarding the Information Technology Department’s responsibility in providing support for personally owned IT equipment (i.e., PC, PDA, notebook, laptop).

6. Remote VPN access will be terminated for any EGSC faculty or staff member who has violated the account credentials guideline (Guideline 2) in this policy and/or Guideline 4 in this policy, which relates to the EGSC acceptable network usage policy.

11.9 Approved Software / Applications Policy

Scope
The software/applications included in this document have been approved for installation on East Georgia State College IT resources. Software/applications found to be installed on college IT equipment that do not appear on this list will not be supported by Information Technology staff and may be removed by Information Technology staff.

If any department (i.e., faculty, staff member) of the College determines that a specific application other than those listed in this policy needs to be purchased, the department must obtain approval from the Vice President for Information Technology prior to purchasing the application. Additionally, in order to determine the application's technical specifications/requirements, the Information Technology Department must be contacted. Furthermore, the Vice President for Information Technology must also sign the departmental purchase request for the specific software/application.

NOTE: Even though a software/application is included in the "approved" listing below, the necessary license must exist (or be purchased) in order for the software to be legally installed on any college-owned IT equipment. Please check with the college's Information Technology Department for more information on software licenses.
Approved software / applications:

Virus protection software:
  1. McAfee Antivirus Software

Word processing and related production software:
  1. Microsoft Office Professional (versions 2007 and higher)
  2. Corel – Word Perfect (version X3 and higher)

Web page authoring software:
  1. Microsoft Front page

Email client software:
  1. Microsoft Outlook & Outlook Express
  2. Campus CatMail system

Internet browser software:
  1. Internet Explorer
  2. Firefox

Diagramming / drawing software:
  1. Microsoft Visio
  2. Microsoft PhotoDraw
  3. Adobe PhotoShop

PDF software:
  1. Adobe Acrobat
  2. Primo PDF

11.10 Campus Email Policy

Scope of Policy
The focus of this policy is to govern the use of electronic mail (Email) communications via the East Georgia State College Email servers and network. To help protect the College's Email and other IT resources from computer viruses, worms, SPAM email, etc., the College utilizes an anti-SPAM firewall (Barracuda 300 Spam firewall) and virus scanning systems (TrendMicro VirusWall Scanner, McAfee Anti-virus software). McAfee Enterprise Anti-virus software is installed on all campus computers, servers and laptops/notebooks.

Regulations of Policy
  1. All Email traffic (incoming and outgoing) that utilizes the East Georgia State College Email server will be scanned by the VirusWall Scanning application and/or anti-SPAM firewall for the following to help protect the College's IT equipment from worms, viruses, Spam Email, etc. This includes the scanning of files attached to email messages. The
contents of messages will also be scanned for items that are known to be related to SPAM Email.

a. File types: .exe, .bmp, .jpeg, .scr, .com, .pif, .zip  Because these file types are known to house viruses, worms, etc., all inbound and outbound Email messages containing attached files with these file extensions will automatically be quarantined by the VirusWall Scanning system. Email messages having valid attached files will be release from quarantine by the Information Technology Department. Please contact the Information Technology Department for assistance with quarantined email messages.

b. Attached files must follow standard file naming conventions of having only one file extension. In other words, no attachment containing more than one period "." in the file name will be allowed.

c. The content of all inbound email messages will be scanned for items associated with SPAM email. These messages will automatically be removed from the email system. The Barracuda Anti-SPAM firewall appliance assists in managing incoming email that is classified as SPAM or "junk" email.

2. Faculty, staff and students who use their East Georgia State College Email account for sending "valid" attached files listed in Regulation 1 should contact the Information Technology department for assistance in proper delivery of the messages via the VirusWall Scanning application.

3. Sending unsolicited email messages via an East Georgia State College email account, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) is prohibited.

4. Any form of harassment occurring via an East Georgia State College Email account, computer system, telephone, paging device or any other form of electronic communication device is prohibited.

5. Unauthorized use, or forging, of email header information is not allowed.

6. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is not permitted.

7. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is not permitted.

8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) is not allowed.

9. Users of the East Georgia State College email system must use their East Georgia State College email accounts only in support of academic pursuits and/or college business.

10. Users of the East Georgia State College email system who suspect their email account has been accessed or utilized by an unauthorized party should contact the College's
11. Because official East Georgia State College communication to students is often sent to students via their East Georgia State College student email accounts, and because the College cannot guarantee the functionality of outside / third-party email systems (i.e., YahooMail, Hotmail, etc), the forwarding of a student's email address to such outside / third-party email systems is not allowed.

12. Report any violations of these policies to abuse@ega.edu or by contacting the EGSC Information Technology Department.

Retention of Electronic Mail

No retention of EGSC email messages (incoming or outgoing) is maintained by the college's Information Technology Department. When users (faculty, staff, students) remove email from the server, no backup of removed messages is maintained. However, a two-week backup tape rotation is maintained for restoring only the operating system and functionality of the email server.

Active Time Period for East Georgia State College Email Accounts and Disclaimers

Student Email Accounts:

a. New students email accounts are created without the request of the student at the time they are accepted for admission to East Georgia State College and before orientation/registration.

b. Readmitted students' email account will not be reactivated until after they have been registered for the returning semester.

c. Student email accounts names are system generated and can only be changed as a result of an official name change. The student must first request an official name change in the Registrar's Office. Once the name change has been processed, the Information Technology Department will create the new email and GA View D2L accounts and transfer any existing “inbox” email messages to the new email account. A “.forward” will temporally be put on the student's old email account for two weeks so that any email going to the old email account will go to the new email account.

Notification that the new accounts are active will be sent to the “old” email account.

It will be the responsibility of the student to transfer any email messages from their sent or other personal folders, including filters and other webmail settings. It is also recommended that the student inform their instructors and other individuals who routinely send them email of their new email account information.

d. Student email passwords are derived from information known by the student. Do not share your password with anyone. Students who believe their password has been compromised may request a password change by either sending a request to cswork@ega.edu using their EGSC email account or in person with proper picture
identification to an EGSC Information Technology staff member at the main campus or at EGSC – Statesboro. If you sent the password change request by email, it is recommended that the student delete the sent email from their sent folder to prevent persons you suspect of having your email password from being able to view the sent message that contains your newly requested password. **Email Password reset requests will not be taken over the phone or from non EGSC email accounts.**

e. It is highly recommended the student preserve their EGSC email account for academic work only. All important college correspondence is sent only to the EGSC email account. This correspondence includes account balance notifications, Mid-Term grades, drop notices, registration notices and pin numbers and test registration information. It is the responsibility of the student to ensure their email inbox has the available space to receive official correspondence.

It is recommended that students obtain other free email accounts (hotmail, yahoo, gmail) for the purpose of subscribing to various mailing lists available on the internet.

f. A student's Email account will be closed and all Email messages deleted for any student who has not attended classes at East Georgia State College for over one year period of time. This time period begins when the student was last enrolled and taking classes at East Georgia State College.

g. Student’s email storage is limited to 30MB of disk space on the email server. Once the disk quota has been reached, the email client will not receive any new mail until the student increases available disk quota by deleting unneeded email messages. It is the responsibility of the student to manage their email storage. Students should do the following to help manage their email storage space.
   i. Check for new mail often
   ii. Delete any unwanted email
   iii. Empty the Trash email folder in the EGSC CatMail system. To empty the Trash email folder, click on the “Empty” option when in the Webmail system. Email is not deleted from the server until the Trash email folder is emptied. Email in the Trash folder will still consume part of the disk quota until the folder is emptied.

h. Additionally, due to disk storage limitations, it may be necessary, WITHOUT NOTICE, for the East Georgia State College Information Technology department to:
   i. Delete email messages that are old (i.e., email messages that are several months in age from date of receipt) from currently enrolled students email accounts
   ii. Delete email containing large attachments.
   iii. Delete email with specific subject line which may have been classified as SPAM that made it through spam filters.

Therefore, it is the responsibility of the student to print out or save to another format any email message that the student wishes to permanently retain.
NOTE: Email that has been moved from the inbox folder into a personal folder in webmail will not be removed. It is recommended that the student move important email out of the “inbox” into a personal folder to ensure it is not deleted.

**Faculty & Staff Email Accounts:**

a. Faculty and Staff email accounts must be requested by submitting a “Network Request Form” which can be found on the EGSC intranet or by going to the following URL: [http://wwi.ega.edu/Forms/network_access.htm](http://wwi.ega.edu/Forms/network_access.htm). If you require assistance in completing this form, please request assistance from Information Technology, Human Resources, your Department Head / Manager or your departmental secretary.

i. Account names will be the first letter of the first name, followed by the first seven characters of the last name when possible.

ii. Password can be requested, but must meet the minimum password standards of: at least six characters in length and include one numeric value and cannot consist of a subset of the account name (i.e., account name asmith with a password of asmith1 or smith1)

iii. Password changes must be requested with the “Network Request Form”.

b. The following SMTP email client is supported by the Information Technology Department: Outlook Web Assess.

c. When a faculty or staff member is no longer an employee of East Georgia State College, the Email account for that faculty or staff member will be closed.

Any person utilizing an East Georgia State College email account who violates any of the regulations listed in this policy is subject to disciplinary action. Please refer to the "Enforcement" section of the *East Georgia State College Acceptable Use Policy* for additional information regarding this issue.

### 11.11 Institutional Website Policy

**Scope of Policy**

East Georgia State College hosts an institutional site on the World Wide Web / Internet to promote the institution, to provide information about the school, and to extend its educational reach beyond the physical campus. Documents placed on the East Georgia State College website must adhere to the following guidelines in order to enhance East Georgia State College’s image as an institution of higher learning.

**Guidelines of Policy**

1.0

a. All pages should be approved by the East Georgia State College webmaster before being placed on the World Wide Web.

b. All pages must not violate copyrights or other restrictions.
c. Production will be limited to faculty/staff authorized to act for their departments/divisions/organizations.

2.0 All pages must:
   a. contain a link to the East Georgia State College home page;
   b. indicate the date of last update;
   c. contain name and e-mail address of person responsible for the page;
   d. contain the full name of department/division/organization in title or document text;
   e. include any navigational aids needed required by the size of documents;
   f. active links to any website mentioned;
   g. present a professional appearance that meets general expectations of an institution of higher learning.

3.0 It is the responsibility of page authors to:
   a. make sure all appropriate copyrights and other restrictions are met before submitting web page for publication
   b. proofread all pages to check spelling and grammar in order to present a professional appearance representative of an organization of higher learning;
   c. check finished document with appropriate browsers;
   d. submit changes and additions to pages to the East Georgia State College Webmaster for prior approval before activating links.

4.0 East Georgia State College reserves the right to remove any content that, in its opinion, violates any of the provisions of this policy.

11.12 Telephone, Equipment, and Software Utilization

Prompt, courteous answers to telephone calls and voice mail messages are very important. Telephone manners should always reflect a professional demeanor. College telephone lines must be kept clear for business use. Personal calls during business hours should be limited and, whenever possible, made during the employee's lunch period. Except in the case of an anticipated emergency, personal cell phones should be on mute or vibrate so as not to disturb others or interfere with work. Excessive personal telephone use will result in disciplinary action. Personal long distance calls may not be charged to the College, as this constitutes a misuse of state funds. Other college equipment, such as fax machines and e-mail are also for college business only. Employees are expected to comply with the Information Technology Policies and Procedures found on the EGSCS intranet and use their college assigned electronic mail account responsibly and in compliance with state and federal laws. All employees shall use software only in accordance with EGSCS’s license agreements. Any duplication of copyrighted software is a violation of federal law and EGSCS policy. Questions regarding software policies for the college may be directed to the Office of Information and Instructional Technology.

Telephones
Local calls are placed by dialing 9 followed by the phone number. Official long distance calls should be placed by dialing 9, the area code, and the phone number. Calls placed to the general
East Georgia State College phone line after 5:00 p.m. are answered by the library staff. A directory of commonly called campus telephone numbers is available in the appendix.

11.13 Computer Lab / Workstation Usage Policy

Scope of Policy
This policy is to provide regulations and information to users of the East Georgia State College computer labs and other campus IT resources. This policy also applies to computer workstations located in classrooms and other public access areas where computer workstations are located. The policy also applies to the utilization of the College's data network via college-owned and non-college-owned IT equipment & devices.

Violators of this policy shall be subject to disciplinary action listed in the "Enforcement" section of the East Georgia State College Information Technology Acceptable Use Policy.

1. Scheduled classes and other official college functions have priority over other uses of computer classrooms. No classes may be scheduled in student computer lab B111 at Swainsboro campus or H134 at EGSC Statesboro.

2. A student must present and have scanned his/her active East Georgia State College Student ID when entering / utilizing the student computer labs listed below. Note: Students are not allowed to use another EGSC student’s ID card.
   - Room B111 at the Student Services Building – Swainsboro campus
   - Room H134 at EGSC Statesboro

2.1 In order to utilize the student computers located in the cyber café area of the Student Services Building, students must enter their East Georgia State College Student ID number (i.e, the number that begins with 9300.)

3. Use of IT equipment located in the East Georgia State College computer labs / computer classrooms are limited to use by EGSC faculty, staff and students. Children are not allowed in EGSC student computer labs or computer classrooms.

4. The student computer labs and computer classrooms are study facilities, so noise should be kept to a low level so as not to disturb others who may be studying. In particular, these are not appropriate places for boisterous behavior or any sort of horseplay.

5. Users of East Georgia State College workstations / computers are not allowed to install software applications on any East Georgia State College workstation / computer.

6. Users of the East Georgia State College network are not allowed to download, copy, or store video files, music files (or related type files) to computers located in the computer labs / computer classrooms or in other EGSC facilities.

7. Food, drink, tobacco products and other similar-type products are not allowed in the computer labs / computer classrooms under any circumstances because they have the
potential for seriously damaging the equipment in the computer labs / computer classrooms.

8. While using an EGSC student computer lab or computer classroom, users may use cellular telephones and other similar communication devices for texting only. Because it can be disturbing to others, cell phone conversations are not allowed inside EGSC student computer labs and computer classrooms.

9. Do not remove paper from the printers located in the EGSC student computer labs / computer classrooms.

10. Do not log into or out of the student computers located in the EGSC student computer labs / computer classrooms. If someone has logged out before you, please restart the computer.

11. Users of the EGSC student computer labs (B111 & H134) who need assistance should contact the Student Assistant in the lab or contact Information Technology Department, which is located in G. L. Smith Building at Swainsboro campus and Room H130 at EGSC Statesboro.