

## **East Mississippi Community College Acceptable Use Policy**

### **1.0 Overview**

East Mississippi Community College's (EMCC) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the College's established culture of openness, trust, and integrity. Restrictions placed on use are to protect the resources and integrity of the network and to comply with all local, state, and federal laws and regulations. EMCC is committed to protecting its students, employees, partners, and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy governs the use of all computers, computer-based communications networks, and all related equipment administered by EMCC. By using these facilities and equipment the user acknowledges consent to abide by this policy. Effective security is a team effort involving the participation and support of every EMCC employee and affiliate who deals with information and/or information systems. It is the responsibility of all users to know these guidelines, and to conduct their activities accordingly.

### **2.0 Purpose**

EMCC is dedicated to providing the best possible services to students, the community, and College personnel and is committed to ensuring that the information system resources are used appropriately for the purposes they are intended. The purpose of this policy is to outline the acceptable uses of computing systems at EMCC. Inappropriate use exposes EMCC to risks including virus attacks, compromise of network systems and services, and legal issues. All computers and network 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 EMCC. These systems are to be used for educational purposes in serving the interests of the institution, and of students and employees in the course of normal operations.

### **3.0 Scope**

This policy applies to students, employees, contractors, consultants, temporaries, and other users at EMCC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned, leased, or authorized for use by the College.

Appropriate use is defined as official business conducted by authorized users. Occasional or incidental use by authorized users for personal, non-business purposes is acceptable, provided that all use is compliant with this policy. The user should be aware that any communications, files or use of EMCC information systems resources are not to be considered private or confidential, regardless of passwords and deletions, and may be monitored, searched and archived at any time. EMCC reserves the right to prohibit access to certain sites, material, and programs. If questions arise as to whether a specific activity complies with appropriate and acceptable use, contact the District Director for Information Technology at [mtvar@eastms.edu](mailto:mtvar@eastms.edu) or 662-476-5059.

### **4.0 Policy**

#### **4.1 General Use and Ownership**

EMCC makes no warranties of any kind, whether expressed or implied, for the services that it is providing. EMCC will not be responsible for any damages suffered by users. This includes, but is not limited to, loss of data resulting from hardware failure, delays, non-deliveries, incorrect deliveries, or service interruptions.

1. Communications should be in a professional manner and not reflect negatively upon EMCC. Do not use vulgarities or any language derogatory toward race, religion, ethnicity, or gender.
2. Email groups have been created to easily communicate business-related information. Refrain from using these addresses for non-business related material.
3. Users are responsible for proper care of computers and equipment and shall not break, disassemble or otherwise cause damage to any computer or equipment.
4. Sharing of resources or access to resources between students, faculty, and staff must be approved by the District Director for Information Technology.

5. Virus email alerts or security threats are often a hoax designed to overload the email system by well-meaning users who forward the email to multiple recipients. If you learn of a virus alert or security threat, report it only to the Information Technology Department for evaluation immediately. Please, do not take any other action. Do not forward the email to other users, and never remove files from your computer as the result of an email.
6. EMCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

#### **4.2 Security**

Important and sensitive data is processed and stored on EMCC computer systems. Usernames and passwords are for the use of the specifically assigned user and are to be protected from abuse or use by others. EMCC has implemented several security measures to assure the safety and integrity of the network and data. Anyone who attempts to disable, defeat or circumvent any security measure will be subject to disciplinary action.

1. Keep passwords secure and do not share accounts. Passwords should be changed at least every two months (60 days). Do not release your password to others. This includes family and other household members when work is being done at home.
2. Because information contained on portable computers is especially vulnerable, special care should be exercised when transporting portable computers.
3. Postings by employees from an EMCC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly those of the user and not those of EMCC, unless posting is in the course of business duties.
4. Do not post your password in a readily accessible area (ex. On monitor, an unlocked desk drawer).
5. Do not leave your computer logged on while not in use.
6. Do not attempt to hack/crack into any systems.
7. Do not use any wireless devices without authorization from the District Director for Information Technology. This includes, but is not limited to, routers, hubs, or modems.
8. Do not create additional domains or workgroups without permission from the District Director for Information Technology.
9. Do not connect any hardware to the EMCC network without prior approval from the District Director for Information Technology.

#### **4.3. Unacceptable Use**

The lists below are by no means exhaustive, but serve as a framework for activities which fall into the category of unacceptable use.

#### **System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violation of any local, state or federal laws while using EMCC equipment
2. Viewing, storing, or distributing obscene, pornographic, or objectionable material
3. Participating in gambling
4. Deliberately propagating any virus, worm, Trojan horse, or trap-door program code
5. Disabling or overloading or attempting to disable or overload any system
6. Attempting to hide your identity or represent yourself as someone else when sending email or any other type of communication
7. Intentionally causing network congestion or significantly hampering the ability of other users to access resources
8. Disclosing any confidential information unless approved by the President or his designee
9. Using computer system resources for soliciting, personal financial gain, partisan political activities, or distributing "junk" email such as chain letters or spam
10. 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 EMCC

11. 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 EMCC does not have an active license
12. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
13. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access,
14. Port scanning or security scanning
15. Executing any form of network monitoring which will intercept data intended for another user
16. Providing information about, or lists of, EMCC students or employees to parties outside EMCC without express permission from the President or his designee

### **Software**

Software programs, including but not limited to, Internet downloaded programs, utilities, add-ins, shareware, freeware, Internet access software, patches, or upgrades, shall not be installed, removed or altered on any desktop, laptop, or server by anyone other than a representative of the Information Technology Department or the Administrative Computing Department without prior approval from the District Director for Information Technology. The software on each computer will be inventoried on a regular basis to ensure compliance. Software owned or licensed by EMCC may not be copied to alternate media except for backup purposes, distributed by email, transmitted electronically, or used in its original form on other than the equipment for which it was licensed. Certain software is strictly prohibited on all computers administered by EMCC. Some of these programs cause a security violation and others degrade the performance of the network.

### **Hardware**

Modifications or additions are not allowed without prior approval from EMCC. Do not relocate hardware unless it is approved by the Information Technology Department and a transfer form has been completed and delivered to the Chief Financial Officer. Information systems equipment should not be removed from the premises of EMCC without express permission from the District Director for Information Technology. Mobile equipment such as notebook computers, projectors, and cameras used in offsite work may be taken off campus only by the person to whom it was assigned.

### **5.0 Enforcement**

All users are required to report any violations of this policy immediately to the District Director for Information Technology.

The Copyright Act of 1976 (amended in 1984) imposes fines up to \$250,000 and up to two years imprisonment for first offenders who have willfully infringed a software copyright. The aim is to deter and punish software criminals. The law also applies to individuals and businesses that misuse copyrighted software. All copyright violations at EMCC should be reported to the District Director for Information Technology so appropriate action can be taken to ensure EMCC is operating within the scope of the law.

Any user who violates this policy is subject to disciplinary action which may include paying for damages, fines, denial of access to technology resources or other remedies applicable under local, state or federal laws or regulations. Employees may also be subject to probation, suspension, or termination. Students may be subject to suspension, expulsion, and other remedies as outlined in school and district policies.

Furthermore, in the event of any illegal activity, the user may also be reported to the appropriate law enforcement authority which may result in criminal or civil prosecution. EMCC will fully cooperate with law enforcement during an investigation.

### **6.0 Definitions**

#### **Term Definition**

**Hack/Crack** – To gain entry to a system to explore, destroy, alter or move data or resources in a way that could cause injury or expense to others, or lead to the gathering of sensitive information.

Network Congestion – An excessive amount of traffic on the network, to the point that messages or other electronic communications are slow or blocked causing network performance to be adversely affected.

Security Compromising Activity – To freely give to unauthorized personnel one's user ID/passwords, EMCC dial-up access numbers, internal IP numbers, or computer or server names, or to install unauthorized software are examples.

Spam - Unauthorized and/or unsolicited electronic mass mailings.

## **7.0 Revision History**

v0.2 - Nov 3<sup>rd</sup>, 2004 (*initial draft*)

v0.3 – Feb 6<sup>th</sup>, 2005 (*2<sup>nd</sup> draft*)