Appropriate Use of Computing and Network Resources

POLICY STATEMENT

Delta State University's computing and network facilities service a large number of faculty, students, staff, and others. In light of the legal responsibilities inherent in the operation of such a system, the University has a number of areas of potential liabilities. This policy sets forth the privileges of and restrictions on students, faculty, staff and other users in respect to the computing and telecommunications systems at Delta State University.

DEFINITIONS

Electronic Communications: The use of computers and network systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools.

Network Systems: Includes voice, video and data networks, switches, routers, wireless devices, and storage devices.

University Computers and Network Systems (University Systems): Computers, networks, servers, and other similar devices that are administered by the university and for which the university is responsible. Throughout this policy, the shortened term "university systems" is used to mean all university computers and network systems.

PROCEDURES and RESPONSIBILITIES

All users have the responsibility to use the University computing systems in an effective, efficient, ethical, and lawful manner. Use of Delta State University's communication resources and computer network is not a matter of right, nor is it provided as a public forum, but rather all use of Delta State University's computer resources and network must be consistent with the mission of the University in support of public education, research, and public service.

GUIDELINES

Security:

- Computer accounts, passwords, and other types of authorization are assigned to individual users and should not be shared with others.
- The individual is responsible for all activities associated with their unique username/ password.
- The user must comply with the University's password policies, quota policies, usage policies, and all University policies.

Academic Freedom:

Free expression of ideas is central to the academic process. However, the University may remove any electronic information from its systems if it is determined that:

- The presence of the information involves illegality (e.g., copyrighted material, software used in violation of a license agreement).
- The information in some way endangers computing, network resources, or the information of other users (e.g., a computer worm, virus, or other destructive program).
- The information is not in compliance with the legal and ethical usage governed by Federal or State law or regulation, or with the University or Institutions of Higher Learning policies.
- The cost of maintaining the information is deemed prohibitive by the responsible administrative unit.
- The user is no longer authorized for access.

Privacy:

It is the policy of the University not to routinely monitor individual use of computing and network resources. However, users should be aware that their use of these resources may not be private. Communications made by means of university computing and network resources are also generally subject to the Mississippi Public Records Act to the same extent as they would be if made on paper. The normal operation and maintenance of the university's computing and network infrastructure require the backup of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service.

The University may monitor the activity and accounts of individual users, including individual login sessions, personal computers, and the content of individual files and communications when:

- The user has voluntarily made them accessible to the public, as by posting to social networking site or posting to a web page or UseNet group;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of computing and network resources or to protect the university from liability;
- There is reasonable cause to believe that the user has violated or is in violation of university policy;
- Or it is otherwise required or permitted by law.

Any monitoring of individual users, other than that allowed by the user or that is necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate Vice President and the Chief Information Officer.

The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual files and communications, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

Inappropriate Usage:

Computing and networking resources should be used only in accord with the guidelines defined in this policy and procedure, all University policies, and state and federal laws. Examples of inappropriate and unacceptable use of computing and networking resources include, but are not limited to:

- Harassment of other users
- Violation of local, state and federal laws, regulations, or policies.
- Destruction of or damage to equipment, software, or data belonging to Delta State University or other users.
- Disruption or unauthorized monitoring of electronic communications.
- Violations of computer system security measures.
- Unauthorized use or attempted use of computer accounts, access codes, passwords, ip addresses, or other network identification words or numbers assigned to others.
- Violation of another user's privacy.
- Academic dishonesty (e.g., plagiarism or cheating).
- Commercial advertising or political campaigning.
- Downloading or displaying obscene or pornographic materials/images.
- Use of computer and/or network facilities in ways that impede the computing activities of others or the University systems, including randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities, overuse of network accessible Internet sites (including gaming, social networking sites, streaming media sites and file download sites) bulletin boards or conferences, and the "off topic" posting of materials to bulletin boards or conferences.
- Use of computing facilities for commercial or business purposes of the user.
- Use of residential network access to conduct business for any purpose is strictly prohibited. Violators will be subject to loss of network services to their residence while a student or resident at Delta State University.
- Violations of trademarks, patents, or copyrights and violation of software license agreements. (Refer to policies of the university.)

- Violation of the usage policies and regulations of the network that Delta State University is a member of or has authority to use.
- Users may not intentionally or negligently disrupt or damage University computers or networks in any way.
- Users of University technology resources may not send electronic messages with the sender's identity forged or send anonymous messages.

Personal use:

Incidental personal use of computing and network resources is permitted, subject to the restrictions outlined in this policy. Personal communications and files transmitted over or stored on University systems and assets are not treated differently from business communications; therefore, there can be no guarantee that personal communications or activities will remain private or confidential.

Sanctions

Violation of the policies described herein for use of computing and network resources are dealt with seriously. Violators may and are subject to the disciplinary procedures of the University, up to and including termination. In addition, violators may lose computing privileges. Illegal acts involving Delta State University computing and networking facilities may also be subject to prosecution by state and federal officials.

Applicable Mississippi Laws that apply to this policy
Mississippi Code of 1972 – http://www.mscode.com/free/statutes/97/045/0011.htm

- Hacking: http://www.mscode.com/free/statutes/97/045/0003.htm)
- Prevention of use: http://www.mscode.com/free/statutes/97/045/0005.htm
- Password cracking/use: http://www.mscode.com/free/statutes/97/045/0005.htm
- Destruction of Equipment: http://www.mscode.com/free/statutes/97/045/0007.htm
- Damaging Information: http://www.mscode.com/free/statutes/97/045/0009.htm
- Intentional Deceit:http://www.mscode.com/free/statutes/97/019/0085.htm
- Sexually oriented materials: http://www.mscode.com/free/statutes/97/005/0029.htm
- Indecent language in a public space (including web spaces) http://www.mscode.com/free/statutes/97/029/0047.htm
- Obscene Materials: http://www.mscode.com/free/statutes/97/029/0101.htm
- Location of Violation: http://www.mscode.com/free/statutes/97/045/0011.htm

RELATED DOCUMENTS

- Digital and Electronic Copyright Infringement
  Commercial Use of University Resources