Alabama State University has implemented a computer usage policy to guide employee and student use of the University's computers & network systems. For questions about this policy, contact the Human Resources Office or the Management & Information Systems Office (IT) at (334) 229-4560.

Read the policy:

ALABAMA STATE UNIVERSITY POLICY REGARDING ABUSE OF COMPUTERS & NETWORK SYSTEMS

The University Computer Abuse Policy applies to all faculty, students and staff. The basic premise is that legitimate use of a computer or network does not extend to whatever an individual is capable of doing with it. Just because you are able to circumvent restrictions or security, doesn't mean that you are allowed to do so.

Violations of the Policy Regarding Abuse of Computers and Network Systems are handled by IST Alleged violations of this policy can be reported directly to MISAC or the ASU helpdesk. If the person responsible is not affiliated with the University, or cannot be identified, the incident should be reported to MISAC or the ASU helpdesk. In addition, some instances may violate federal law.

EXAMPLES (NOT A COMPREHENSIVE LIST) OF POLICY VIOLATIONS INCLUDE:

- ❖ Accessing, or attempting to access, another individual's data or information without proper authorization (e.g. using someone's net id and password to look at their personal information)
- ❖ Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained (e.g. password sharing)
- ❖ Tapping phone or network lines (e.g. running network sniffers without authorization)
- ❖ Making more copies of licensed software than the license allows (i.e. software piracy)
- ❖ Sending a crippling number of files across the network (e.g. e-mail "bombing")
- ❖ Releasing a virus, worm or other program that damages or otherwise harms a system or network
- ❖ Preventing others from accessing services (e.g. taking over a chat channel and kicking other users off)
- ❖ Unauthorized use of University resources (e.g. using someone else's remote dial-in access or borrowing their net id and password to access the library systems)
- ❖ Sending forged messages under someone else's net id (e.g. sending hoax messages, even if intended to be a joke)
- ❖ Using University resources for unauthorized purposes (e.g. using personal computers connected to the campus network to set up web servers for illegal, commercial or profit-making purposes)
- ❖ Unauthorized access to data or files even if they are not securely protected (e.g. breaking into a system by taking advantage of security holes)

- ❖ Initiating or encouraging the promulgation of chain letters and other types of electronic broadcast messages, tapping phone lines or other network cables, subverting or obstructing a computer or network by introducing a worm or virus, supplying false or misleading information to access computer or network systems, improperly obtaining or using someone's password to access computers or network systems, and unauthorized access to data, computers or networks.

RESPONSIBLE USE OF ELECTRONIC COMMUNICATIONS

This policy applies to the entire Alabama State community. It attempts to deal with some of the newer problems resulting from widespread use of the Internet. As stated in the policy, the University cherishes the diversity of values and perspectives endemic in an academic institution and is respectful of freedom of expression. Therefore, it does not condone censorship, nor does it endorse the inspection of files other than on an exceptional basis. As a result, the University cannot protect individuals against the existence or receipt of material that may be offensive to them. The University encourages individuals to use electronic communications in a responsible manner. Finally, the policy includes information about behavior that would constitute a violation and contains a set of procedures for reporting incidents.

Policy violations fall into four categories that involve the use of electronic communications to:

- ❖ Harass, threaten, or otherwise cause harm to specific individuals, for example, sending an individual repeated and unwanted (harassing) e-

mail or using e-mail to threaten or stalk someone; Alleged violations of this type can be reported directly to **Management & Information Systems (MIS)** or to the **Alabama State University Department of Public Safety** if the situation is potentially serious and requires immediate attention. If the person responsible is not affiliated with the University or if it is not possible to identify the individual, the incident can still be reported to the police. These offices can assist by referring to appropriate sources of help outside the university. Save electronic copies of all correspondence for evidence.

❖ Impede, interfere with, impair, or otherwise cause harm to the activities of others, for example, propagating electronic chain mail, or sending forged or falsified e-mail; Alleged violations of this type can be reported to **Management & Information Systems (MIS).** If the person responsible is not affiliated with the University, the incident should be reported to the site that provides the individual with Internet access. If it is not possible to identify the origin, **contact MIS** for assistance. Save electronic copies of anything that can be used as evidence.

❖ Download or post to University computers, or transport across University networks, material that is illegal, proprietary, in violation of University contracts, or otherwise is damaging to the institution, for example, launching a computer virus, distributing pornography via the web, or posting a University site-licensed program to a public bulletin board; Other examples include information dealing with cults or the occult, hacking, hate speech, nudism and naturalism, peer to peer file sharing, adult

pornography, sexual orientation, and weapons. Alleged violations of this type can be **reported directly to MIS**. If the person responsible is not affiliated with the University, or cannot be identified, the incident should still be reported to MIS.

❖ Harass or threaten classes of individuals; Alleged violations of this type can be reported directly to the **Human Resources Office**. If the person responsible is not affiliated with the University, the incident should be reported to the site that provides the individual with Internet access. If it is not possible to identify the origin, **contact MIS** for assistance. Save electronic copies of anything that can be used as evidence.