ARKANSAS STATE UNIVERSITY - NEWPORT
NEWPORT • JONESBORO • MARKED TREE

ASUN Operating Procedure – 6001

Operating Procedure Synopsis

Title: Appropriate Use of IT
Approval Date/Revision Date(s):
Review Date(s): 7/2018, 7/2019, 7/2020, 7/2021, 7/2022
Executive Cabinet Liaison: Vice Chancellor for Finance and Administration
Responsible Operating Procedure Manager: Director of IT

A. Purpose and Scope

The purpose of this policy is to ensure an Information Technology Services infrastructure that promotes the basic missions of the institution in teaching, learning, and administration. In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT systems
- To ensure that use of ITS systems is consistent with the principles and values that govern the use of other institution facilities and services
- To ensure that ITS systems are used for their intended purposes
- To establish processes for addressing policy violations and sanctions for violations

This policy applies to all ASUN users including but not limited to students, faculty, and staff. It applies to all ITS systems which includes services, networks and facilities that are administered by the ITS department. Use of the ITS systems even when carried out on a privately owned computer or other device that is not owned by ASUN is governed by this policy.

B. Definitions

Computer resource – a device connected to the network

Integrity – assurance that information can only be accessed or modified by those authorized to do so

Copyright – form of protection provided by the laws of the United States to authors of "original works of authorship"

User – any person, whether authorized or not, who makes any use of any ITS system from any campus of Arkansas State University-Newport

C. Procedures

1. RIGHTS AND RESPONSIBILITIES

*All ASUN students, faculty, staff and administrators are expected to adhere to operating procedures.

ASU-Newport expects that users of campus computing and network facilities will respect the rights of other users as well as the integrity of the systems and related physical resources. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws. Because ASU-Newport is a state agency, all information stored in computers owned or operated by ASU- Newport is presumed to be a public record and subject to disclosure under the Arkansas Freedom of Information Act unless exempt under the law. Users do not own accounts on college computers, but are granted the privilege of exclusive use. While users are entitled to privacy regarding information contained on these accounts, the Electronic Communications Privacy Act authorizes system administrators and other university employees to access user files. By utilizing ASU-Newport computing and network resources, you give consent to accessing and monitoring by system administrators and other university employees of any electronic communications, including stored communications, in order to enforce this policy or to protect the integrity of computer systems or the rights or property of the university. System administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law. In addition, student files on university computer facilities are considered education records under the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. Section 1232(g)).

2. ENFORCEMENT

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the person administering the accounts or network. This may be done through electronic mail or in-person discussion and education. Repeated minor infractions or misconduct that is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. In addition, offenders may be referred to their sponsoring advisor, department, employer, or other appropriate college office for further action. If the individual is a student, the matter may be referred to the Office of Student Services/Financial Aid for disciplinary action. Any offense that violates local, state, or federal laws may result in the immediate loss of all college computing privileges and will be referred to appropriate university offices and/or other law enforcement authorities.

3. STANDARDS

Conduct that violates this policy includes, but is not limited to, the activities in the following list:

- Unauthorized use of a computer account.
- Using the campus network to gain unauthorized access to any computer systems.
- Connecting unauthorized equipment to the campus network.
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage, or to place excessive load on a computer system or network. This includes, but not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Deliberately wasting/overloading computer resources, such as printing too many copies of a document, using the Internet, radio, playing games, watching movies, or using file sharing applications (Peer-to-Peer) for personal use.
- Violating terms of applicable software licensing agreements or copyright laws.

• Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
• Using university resources for commercial activity such as creating products or services for sale.
• Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
• Initiating or propagating electronic chain letters.
• Inappropriate mass mailing. This includes multiple mailings to news groups, mailing lists, or individuals, e.g. (spamming, flooding, or bombing).
• Forging the identity of a user or machine in an electronic communication.
• Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing laws or university regulations.
• Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.
• Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

D. Related Information