



Policy # 56005

COMPUTER USE POLICY

Effective Date: October 18, 2002

Revised Date: February 6, 2023

Responsible Office: Information Technology

Division: Operations

I. PURPOSE

To define acceptable and unacceptable computer use practices, to promote an understanding of responsible usage of university computing resources, and to protect and conserve those computing resources. This policy will follow the guidelines of the Office of Information Technology (OIT) IT-POL-005.

II. STATEMENT OF POLICY

The computing facilities at Grambling State University are provided for the use of GSU students, faculty, staff and authorized persons in support of the programs of the University. All students, faculty and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner.

- A. Computer facilities and accounts are owned by the University and are to be used for university-related activities only. All access to central computer systems, including the issuing of passwords, must be approved through the Information Technology Center. All access to departmental computer systems must be approved by the department head or an authorized representative.
- B. Computer equipment and accounts are to be used only for the purpose for which they are assigned and are not to be used for commercial purposes or non-university related business. Incidental use of computer communications facilities by members of the faculty and staff for the purpose of creating and maintaining job efficiency and harmonious working relationships is consistent with this policy.
- C. An account assigned to an individual by the Information Technology Center or a department must not be used by others without explicit permission from the instructor or administrator requesting the account and by ITC or department assigning the account. The individual is responsible for the proper use of the account, including proper password protection.
- D. Students and employees should have no expectation of privacy when utilizing university computing resources. The university reserves the right to inspect, without notice, the contents of computer files, regardless of medium, the

contents of electronic mailboxes, systems output such as printouts, and to monitor network communication when it is considered reasonably necessary to maintain or protect the integrity, security or functionality of university or other computer resources or to protect the university from liability; there is reasonable cause to believe that the user has violated the Computer Use Policy or otherwise misused computing resources; an account appears to be engaged in unusual or unusually excessive activity; or, it is otherwise required or permitted by law.

Such inspection or monitoring may be conducted only by authorized personnel for compelling business or security reasons and only with the approval of the President or the following designees: for faculty members, the Vice President for Academic Affairs; for staff members, the Vice President for Finance or for students, the Vice President for Student Affairs.

- E. Electronic communications facilities (such as electronic mail, university webpage, mobile devices, notebooks, desktops, etc.) are for university-related activities only. Fraudulent, harassing, or obscene messages and/or other materials are not to be posted, sent or stored.
- F. No one may deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any university computer system.
- G. Loopholes in computer security systems or knowledge of a special password must not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems, or use systems for which proper authorization has not been given.
- H. Materials protected by copyright are not to be copied from, into, or by using campus computing facilities, except as permitted by law or by contract with the owner of the copyright. This means that such materials may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of the copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department. Materials would include, but not be limited to software, audio, image, video, and test data.
- I. All licensed computer software must be installed by Network Services or by an approved designee as identified in the college or administrative division. Once the software is installed, administrative privileges on the computer will be disabled. **The installation and use of unlicensed computer software is in violation of university policy.**
- J. Computer equipment must be configured by Network Services to use the power Management features of the operating system to place the monitor and hard drive in “sleep” mode after a period on inactivity no greater than sixty (60) minutes.

- K. Violations of the policies will be dealt with in the same manner as violations of other university policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the University, and legal action.