GRAMBLING STATE UNIVERSITY NETWORK POLICY

Effective Date: December 2011   **Revised Date:** February 6, 2023
Responsible Office: Information Technology Center
Division: Operations

I. PURPOSE/OBJECTIVE

The Grambling State University network is used to transmit information and is vital in carrying out the mission of the university. This policy is to define the guidelines to maintain the integrity of the university's network to conduct communication. This policy is a supplement to the following Information Technology Center's policies: #56005 Computer Use Policy, #56006 Electronic Communications Policy, #56004 Password Policy.

II. STATEMENT OF POLICIES

The Information Technology Center is solely responsible for providing a reliable and secure network infrastructure for the university. To maintain network performance and maximize the availability of service, the guidelines in this policy are for appropriate use of the university's network.

A. All equipment used on the university's network must be within university standards, meet current industry standards, and be approved by the Associate Vice President for Information Technology pursuant to the Information Technology Procurement Policy.

B. Network equipment should be configured, modified, and limited to Information Technology Center's Network Services or authorized personnel.

C. Devices should not be added to the network by unauthorized personnel that will impair the usability or performance of the university's network. The Information Technology Center will disconnect any device(s) that interferes with the network performance, unauthorized device(s) or device(s) that violate the network security.

D. Each individual is assigned an id and password for the university's network. Each user is responsible for the use of their network id and password. The Information Technology Center reserves the right to remove access when university policies, state or federal laws have been violated.

E. The Information Technology Center reserves the right to monitor information transmitted on the network to investigate performance or system issues, search for viruses or other harmful programs, or search individual login sessions and files to determine if this policy is being violated.

F. To maintain the security of the network, the Information Technology Center's Network Services will apply patches, anti-virus software and provide monitoring for the network.

G. The Information Technology Center will be responsible for reporting any breaches of this policy to the respective Vice President.

III. NON-COMPLIANCE or DISCIPLINARY ACTION

A. Violation of this policy by any individual or groups which adversely affects the university's network services will be subject to institutional disciplinary action. Violators will be subject to the normal disciplinary procedures of the University. Students will be subject to applicable student discipline, faculty will be subject to applicable faculty discipline, and staff will be subject to applicable staff discipline. Any such discipline may include, in the case of students expulsion from the university or in the case of faculty and staff termination of employment.

B. Any users, including students, faculty, and staff, provided University network access who violate this policy privileges or access may be suspended. Devices that adversely affect the university's network services may be confiscated and not returned to the violator.

C. Appeals to any disciplinary action shall be in accordance with the disciplinary policies as outlined in the student, faculty, or staff handbook as appropriate.