



## Policy Directory

Responsible Division: Finance and Administrative Services  
Responsible Office: CITS  
Issue/Revision Date: 12/01/2017

## **Wireless LAN (Wi-Fi) Access Policy**

---

---

Policy:

### **SUMMARY**

The Alcorn State University Wireless LAN (named as Wi-Fi network) is provided to facilitate and support teaching, academic activities and job related duties required in the University.

The Wi-Fi network is part of the Campus Network which is managed and administered by the Center for Information Technology Services, Alcorn State University. Use of the Wi-Fi network is governed by the guidelines and policies described in this document.

### **POLICY STATEMENT**

#### **1. Proper Use**

Wi-Fi network users should ensure their computer systems are properly configured and operated so that they do not cause inconveniences to other Wi-Fi network users and the campus network users.

- a. The Wi-Fi network is provided in support of teaching or related academic activities to access Campus Network and Internet in lecture theatres, classrooms and libraries. Use of the Wi-Fi network for other purposes should be discussed with and approved by the CIO.
- b. Wi-Fi network users should get their network addresses automatically; a valid network address will be granted when connected. Use of other network address is prohibited.
- c. Setting up routing or other special network functions is prohibited.
- d. Servers set up for the provision of ftp/web/banner/blackboard services for campus users are allowed subject to the following conditions:
  - i. No extensive loading that affects the performance of the campus network, nor monopolization of the campus network resources in terms of bandwidth. Server connections that violate these guidelines will be terminated without further notice.
  - ii. For the support of teaching, research and student services
  - iii. Not to harm the campus network. CITS reserves the right to prohibit the running of other servers which are harmful to the network (e.g. system services such as DHCP)

#### **2. User Rights and Responsibilities**

Wi-Fi network users have the following rights and responsibilities:

- a. Producing excessive network traffic such as broadcasting and sending massive messages and unsolicited emails is prohibited.
- b. Setting up routing or other special network functions is prohibited.
- c. Development of networking software in the Wi-Fi network is prohibited.
- d. Sharing of accounts is prohibited.
- e. Users are responsible at all time for using the Wi-Fi network in a manner that is ethical, legal, and not to the detriment of others.
- f. Users are responsible for the licenses of the software installed in their computer.
- g. Users are responsible for any and all activities initiated from their computer.
- h. Users are responsible for the security settings of their computer or notebook systems.
- i. Users have the right to access the campus network and Internet and use applications including e-mail, WWW, news and etc.
- j. Users of the Wi-Fi network whom violate the terms and conditions set forth in this document will result in temporary or permanent loss of the access privilege to the Wi-Fi network. Offences which are in violation of law usually will result in immediate loss of access privilege of the Wi-Fi network and will be reported to the appropriate University or law enforcement authorities.
- k. Users should take extra cautions when using the University Wi-Fi service.

### **3. CITS Staff Rights and Responsibilities**

- a. CITS staff is responsible for the design, operation and management of the Wi-Fi network, including provision of security measures at the network level.
- b. In the event of severe network problem which arises from the Wi-Fi network user's computer system and causing severe damage to the University user community, CITS staff has the right to terminate the network connection of the user's computer system without making prior notice to the user.
- c. The CITS staff has the responsibility to provide advance notice of the Wi-Fi network's unavailability due to regular maintenance, upgrades or changes so that Wi-Fi network users may plan for their works. However, in the event of an emergency, the CITS staff has the right to shut down the whole or partial Wi-Fi network with little or no advance notification. Every effort will be made to give users a chance to save their work before the Wi-Fi network is taken out of service. In the event that a Wi-Fi network connected computer presents an immediate security risk to equipment, software or data in campus network, CITS staff has the right to terminate this connection without prior notice.

### **PROCEDURE**

Wi-Fi network users violating the guidelines and policies set forth in this document may result in temporary or permanent loss of the access privilege to the Wi-Fi network. Offenses which are in violation of local laws usually result in immediate loss of access privilege to the Wi-Fi network, and will be reported to the appropriate University and law enforcement authorities.

**CONTACT INFORMATION**

Contact the CITS department for more information: (601) 877-6182.