WIRELESS POLICY

Introduction

The Wireless Usage Policy applies to all computers, laptops, local area networks, wireless, servers, systems, and application software packages used on campus. It also applies to all staff, faculty, and students at UAPB. The purpose of this policy is to ensure the security, reliability, and utilization of the wireless network.

Wireless Network and Internet access are available at the University of Arkansas at Pine Bluff campus. Due to the nature of wireless communication, wireless networking requires increased cooperation between faculty, staff, and students to maximize the benefits of this technology.

Purposes

The purpose of this policy is to inform users of the acceptable use of regulations related to UAPB's wireless network. This policy has been put in place to protect the staff, faculty, and students and to prevent inappropriate use of wireless network access that may expose UAPB to multiple risks, including viruses, network attacks, and various administrative and legal issues.

This policy has been created to expand on the Acceptable Use Policy by including specific information regarding the use of wireless networking and data access on campus.

This policy is subject to change as new technologies and methods of implementing these technologies emerge.

General Use

It is the intention of IT to provide a high level of reliability and privacy when using the wireless network. Wireless access points distributed around the campus to provide and maintain availability. Wireless access points provide a shared bandwidth, and so as the number of users increases, the available bandwidth per user decreases. As such, users are asked to be considerate of other users and refrain from running high bandwidth applications and operations such as downloading large music files and videos from the internet.

The level of user traffic and accessibility determines network reliability. The level of security and regulation of bandwidth is according to user role and location. UAPB cannot guarantee the confidentiality of any information stored on any device connected to the UAPB Wireless Network; therefore, the wireless network should not be used to transmit critical and sensitive information, such as social security and credit card numbers. Individuals assume full responsibility for their actions.

Coverage

The UAPB Wireless Network is located throughout most of the campus. IP tunneling is unavailable at this time, and so users may need to reconnect when traveling from building to building. The availability of IP tunneling is subject to change as the requirements of users continue to be assessed. Technical Services Director and Network Administrator approve all wireless access points across campus.

Access

Access to the UAPBWireless by Students, Staff, Faculty, and Guest will need to authenticate after joining the SSID by opening a browser to be directed to the login page. By connecting to the UAPB wireless networks, you agree to the terms of use addressed in this policy and the Acceptable Use Policy at the login screen.

Security

Wireless Networks are insecure and can be unsafe. The security features of Open WEP (Wired Equivalency Protocol) are imperfect and allow for eavesdropping or "sniffing" of wireless traffic to potentially capture all traffic that is not encrypted with a third-party product.

Eavesdropping on any UAPB network communication (wired or wireless) is illegal and a violation of the UAPB Acceptable Use and Wireless Usage policies. All violations will result in disciplinary action.

All computers connected to the UAPB network, whether owned by the employee, student, or UAPB, is strongly recommended be running approved anti-virus software with the latest virus updates.

For security and network maintenance purposes, IT may monitor individual equipment or wireless network traffic at any time. UAPB reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Technical Services has the power to disconnect any device from the wireless network that violates the practices outlined in this policy or any other linked policy. It is the responsibility of the user to be aware of the information described in such systems.

All Authorized Users, Guests, and Students are responsible for the following:

- Adhering to established networking guidelines and policies.
- The implementation of antivirus and firewall type of security software, patches, and protocols on any equipment used to access the UAPB Wireless Network.
- Compliance with all university policies and procedures and with local and state legislation on the security of sensitive and confidential data on campus networks.
- Reporting known violations of the wireless network and all related equipment to IT. Violations

Any violations of the rules put forth in this policy may result in the following disciplinary actions being taken by the University:

- Restricting a person’s access to some or all of the university resources.
- Criminal prosecution under state and federal laws.