Wireless Access Policy

Purpose and Scope
The goal of this policy is to protect Southeast Arkansas College’s technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to our public image. All users employing wireless methods of accessing SEARK technology resources must adhere to SEARK College defined processes for doing so, using the College approved access points. Unauthorized access to the wireless network is not allowed.

Wireless networks are not a replacement for a wired network. As the College’s wireless network is an extension to the existing wired network, wireless access should not be used for work sessions that require the transfer of large amounts of data (e.g., backups or file downloads) or for access to sensitive organizational data.

The following policy is complementary to any previously implemented policies dealing specifically with network access and remote access to the enterprise network.

Supported Technology
Southeast Arkansas College uses the 802.11b/g/n protocols as its wireless network standard, transmitting at the 2.4 GHz radio frequency spectrum, with the intention of internet access only to mobile and wireless devices.
In order to provide wireless access to authorized users, Information Technology (IT) must install "access points" in and around the campus. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g. PDA, laptop, etc.), which then converts the radio signal back to a digital format the mobile device can use.

"Rogue" access points are antennas that are installed without the knowledge or permission of Southeast Arkansas College, used by individuals to gain illegal access to the College’s network.

Southeast Arkansas College supports the following devices and equipment for accessing our network and systems wirelessly:

- Access Points installed by the Information Technology (IT) department
- Laptop computers using Windows Vista/7/10, Linux or Mac OS X 10.4.11 and above
- Cellular phones, tablets, and other devices which support the ability to sign in on the device.

**Policy and Appropriate Use**

All wireless access points within the College’s firewall must be approved and centrally managed by SEARK College Computing Services Department (Information Technology Division). The addition of new wireless access points within campus facilities will be managed at the sole discretion of IT. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment on campus premises, are strictly forbidden.

The IT department will occasionally conduct sweeps of the wireless network to ensure there are no rogue access points present.

The IT department reserves the right to turn off without notice any access point connected to the network that it feels puts the College’s systems, data, and users at risk.

All wireless clients and devices shall be required to be fully patched and have installed the anti-virus software. The user shall update these applications as required, and will not reconfigure them in any way. 802.11 access point broadcast frequencies and channels shall be set and maintained by the IT Department. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

All computer equipment and devices used to connect to the College’s network must display reasonable physical security measures. Users are expected to secure their College-connected devices when they are physically at their machines as well as when they step away.
Wireless access users agree to immediately report to the SEARK College IT department any incident or suspected incidents of unauthorized access point installation.

Use of the wireless network is subject to the same guidelines as the Southeast Arkansas College Computer Use Policy.

Any questions relating to this policy should be directed to epolicy@seark.edu.

Policy Non-Compliance
Failure to comply with the Wireless Access Policy may result in the suspension of wireless access privileges and possible disciplinary action.

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Revised Date</th>
<th>Author/ Editor</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>February 22, 2016</td>
<td>JoAnn Dupra</td>
<td>Initial policy created.</td>
</tr>
</tbody>
</table>