ASUN Operating Procedure – 6004

Operating Procedure Synopsis

Title: Deployment of Wireless Network
Approval Date/Revision Date(s):
Review Date(s): 7/2018, 9/2019, 9/2020
Executive Cabinet Liaison: Vice Chancellor for Finance and Administration
Responsible Manager: Director of IT Services

A. Purpose and Scope

Arkansas State University-Newport ensures compliance with all wireless networks for protecting the institutions assets, information systems, and IT resources from unauthorized access or damage. This process is also to maintain the confidentiality, integrity and availability supporting the mission and functions of the institution.

B. Definitions

Access point – device that allows wireless devices to connect to a wired network using Wi-Fi or related standards

Wireless network – any type of computer network that uses wireless data connections for connecting network nodes

Wired network – connects devices to the Internet or other network using cables

C. Procedures

Wireless networks are layered on all wired networks at Arkansas State University-Newport. Any device utilizing access to the institutions network infrastructure is subject to the following:

1. All use of wireless access points and devices must comply with applicable laws, regulations, and university policies including FCC regulations and the institution's provisions for Acceptable Use.
2. Only centrally managed, institution-owned wireless access points may be attached to any Arkansas State University-Newport network.
3. Any wireless access point and device providing access to data identified as "Restricted" in the data classification manual must support data encryption of identified data while in transit and must not retain any data in such manner.
4. Any wireless access point or device must utilize IP address space as assigned by network management via a static or dynamic address assignment.

Enforcement – The Information Technology Services department will notify personnel operating a wireless access point or device that does not appear to be compliant with the process so that it may be removed from the network. In a perceived emergency situation, the ITS department may take immediate steps, including denial of access, to ensure the integrity of the institution's data network and systems, safeguard the health and safety of the institution community members' and property, or protect the institution from liability.

D. Related Information

All of the Information Technology Services policies and procedures will be available on the portal under the Information Technology Services tab.