WASHINGTON STATE UNIVERSITY'S WIRELESS LAN POLICY

BACKGROUND

The use of Wireless LAN's for data communications offers increased flexibility and mobility over wired solutions. Due to this the requirement for wireless access throughout the campus is expected to dramatically increase over the next few years. At the same time the technology presents the following challenges:

- ***Shared Spectrum***
  Wireless data networks using the IEEE 802.11 specification operate in the 2.4 GHz or 5 GHz radio spectrums. Both frequencies must be shared by all applications utilizing them in the same coverage area. This can be a problem if adjacent departments in the same building or area independently operate wireless LAN's. Problems may also be caused in the 2.4 GHz spectrum by other competing applications such as microwave ovens or some cordless phones.
- ***Non-Overlapping Channels***
  Both frequencies are limited by the number of non overlapping channels that are available with the 2.4 GHz frequency limited to only 3 non overlapping channels and the 5 GHz frequency limited to 20 non overlapping channels.
- ***Security***
  Most of the security schemes that are currently available are easily compromised.

For the above reasons the following policies are necessary:

POLICIES

1. ***Management***
   To ensure the technical coordination required to provide the best possible wireless network for Washington State University, Information Technology's Communications Group or the Information Services departments at the Newer Campus locations will be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the campus. Departments should not deploy 802.11 or related wireless standards access points without coordination with the appropriate IT Group.

2. ***Deployment***
   Wireless access will be deployed in a manner such that access meets the greater needs of the campus and usage will not be restricted to a specific use and/or department.

3. ***Equipment***
   In order to maintain compatibility between the various components of the Wireless LAN and to provide spare equipment in case of failure, IT's Communication Group or the Information Services Departments at the Newer Campus locations will specify the equipment to be used in the Wireless LAN.

4. ***Security***
   All wireless access will be connected to authentication services through the use of a VLAN to an authentication service. Unauthenticated access to services on the WSU LAN will not be permitted. In addition all access will be through a VPN gateway in order to secure and encrypt wireless communications.

5. ***Non Compliance***
   Due to the shared nature of the wireless spectrum and the need for security, equipment already in place that interferes with approved equipment or that does not comply with the security requirement will need to be modified or replaced. The appropriate IT group will work with the owner of the equipment to rectify the situation, however if a solution can't be reached the equipment may be disconnected. Departments who are planning new installations should ensure that they work with the appropriate IT group to avoid these issues.