1. **Purpose**

1.1. The purpose of this policy is to establish the standards and guidelines under which mobile devices such as laptops, mobile phones, PDAs and handheld computing devices may access the university’s wireless network.

2. **Scope**

2.1. This policy applies to all users of Weber State University information technology resources regardless of affiliation and irrespective of whether those resources are accessed from on-campus or off-campus locations.

3. **References**

3.1. PCI DSS Requirements 2 and 12

3.2. ISO 17799 Sections 10 and 11

4. **Definitions**

4.1. *Modem* – A device that encodes digital signals into analog signals and vice versa for sending data over a telephone line.

4.2. *Wireless Access Point* – A device that serves as a common connection point for computing devices in a wireless network or a device that allows a network router to connect to another network using antennas for access by multiple users.

4.3. *Wireless Network* – A local area network technology that uses radio signals to connect computing devices to the university’s wired network.

4.4. *Network* – The interconnection of two or more computers that may share files, folders, applications, or resources such as file servers, application servers and printers.

4.5. *User* – All faculty, staff, administrators, students, consultants and any person or agency employed or contracted by the university or any of its auxiliary organizations who have a legitimate need to access the University network.

4.6. *Critical IT Resource* – An IT resource which is required for the continuing operation of the institution and/or its colleges and departments, including any IT Resource which, if it fails to function correctly and/or on schedule could result in a major failure of mission critical business functions, a significant loss of funds or a significant liability or other legal exposure.
4.7. Information Technology Resource (IT Resource) – A resource used for electronic storage processing or transmitting of any data or information, as well as the data or information itself. This definition includes, but is not limited to, electronic mail, voice mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications and any computer facilities or related electronic equipment that electronically stores such communications.

4.8. Service Set Identifier (SSID) – The name used to broadcast the wireless signal carrying the name of a network.

4.9. Spectrum – 2.4 and 5 Gigahertz unlicensed 802.11

5. Policy

5.1. Weber State University has provided a robust wireless network to campus users to facilitate connection to the University IT resources. In order to effectively manage the university’s wireless infrastructure, to ensure connectivity without interference and guard against malicious or unauthorized access to the University network all users are required to abide by the standards set forth in this policy.

6. Standards

6.1. All users of the university’s wireless network must comply with University policies, in particular PPM 10-2, Acceptable Use Policy, and all federal, state and local laws.

6.2. Desktops, non-mobile laptops, printers and other stationary computing equipment will not be granted access to the WSU wireless network. Any requests for exceptions to this section of this policy will be considered on a case by case basis and should be submitted via email to the appropriate WSU network administrator.

6.3. Access to the Internet through the secure wireless network will only be permitted through authorized and proper authentication.

6.4. To ensure proper network location, wireless access points used for connecting to the university’s network shall only be installed by a member of the Information Technology Division (ITD) or their designee in accordance with the System Configuration Standards and with the approval of the VP for Information Technology. All access points must be labeled with the owner’s name, contact information and purpose.

6.5. Separate deployments of wireless access points for academic purposes must be coordinated with the ITD to avoid interference and duplication. Wireless access points
deployed by others which create radio frequency interference with the university’s wireless service or duplicate existing wireless services will be disconnected from the network.

6.6. It is the responsibility of the ITD designee to ensure temporarily approved academic wireless access points are regularly monitored and removed at the end of each semester or at the end of the approved period.

6.7. Students are strictly prohibited from being administrators for academic wireless networks.

6.8. Only ITD approved wireless access points shall be allowed to broadcast from standard University SSIDs. All others are prohibited from installing wireless access points for the purpose of providing access to the university’s wireless or wired network or to extend the coverage areas of the University’s wireless network.

6.9. A list must be maintained of all approved wireless access points.

6.10. A list of University approved products for wireless access is available through the ITD.

6.11. All critical IT resources shall require authentication (User IDs and passwords, tokens, VPNs, etc.) to protect against malicious or other types of unauthorized access to the university’s information technology resources.

6.12. The use of modems to connect to the University network is strictly prohibited.

7. Exceptions

7.1. Exceptions to this policy must be approved by the ISO with review by the Information Security Task Force.