Wireless Access Points Policy

Applies To:	All	Policy Number:	ITS-0033
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	July 1, 2016	Last Review Date:	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope
This policy covers all devices that provide wireless access to the University network or wireless access within University property.

Purpose
Devices that provide wireless access to a network are commonly referred to as wireless access points or wireless routers. These devices may create a security risk by providing unauthorized access to University resources, including the disclosure of University protected data.

Improperly configured devices or devices added without consideration to the University master wireless plan congest the airwaves and significantly slow down the overall performance of the University's wireless services.

Policy
All members of the University community are prohibited from attaching any device operating as a wireless access point or router in any University building. ITS is the sole provider of wireless access points throughout the University's indoor and outdoor air space.

Any wireless connectivity into the PCI-DSS environment is strictly prohibited. Wireless networks are not allowed to connect to the credit card processing (High Security Network) environment under any circumstances.

When Information Technology Services (ITS) becomes aware of any problem that involves a device operating as a wireless access point that is attached to the campus network in violation of this policy, the network connection to the device will be severed and the "best known" responsible entity will be asked to remove the unit. If the unit is accessible to ITS, ITS has the right to turn the unit off. If additional attempts to reconnect a prohibited device to the campus network are made, the matter will be referred to the appropriate University disciplinary staff.

History and Updates
July 1, 2015: Initial Policy