Wireless Communications Policy  
COE–WCP–01

1.0 Purpose
This policy establishes procedures for gaining secure access to wireless data communications on the College of Engineering’s networks. Only College maintained wireless systems that meet the criteria of this policy are approved for connectivity to the College of Engineering's networks. No personally procured, installed or maintained wireless routers are permitted for use on any College network.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, PDAs, Phones, etc.) connected directly to any of the College of Engineering's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the College of Engineering’s networks do not fall under the purview of this policy.

3.0 Policy
The College of Engineering installs, operates and maintains state-of-the-art secure wireless communications networks in its academic buildings, thereby providing unrestricted network access to College resources by Engineering faculty, staff and students. Non College faculty and students have the ability to connect to the wireless networks in Engineering buildings but are restricted from gaining access to College resources; rather, their communications are tunneled directly to the Penn State backbone.

Wireless access points that are not installed, operated or maintained by the College's central IT staff shall be considered as rogue AP and once detected will be blocked from communicating on/across the College backbone. All wireless users are bound by University and College communications and computing policies pertaining to systems operations, scanning of systems for Privately Identifiable Information (PII), Digital Copy wright Millennium Act (DCMA), Virus protection and restriction on scanning on the network. ECS managed College Email and Virtual

4.0 Enforcement
Local wireless networks failing to comply with this policy will be disconnected from the College network; their hardware’s MAC address will be blocked at the network level. Furthermore, any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

5.0 Definitions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Authentication</td>
<td>A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access (WPA) is a security protocol for wireless 802.11 networks from the Wi-Fi Alliance that was developed to provide a migration from WEP</td>
</tr>
</tbody>
</table>

6.0 Revision History
Last updated: 12/1/10