## Wireless Policy

<table>
<thead>
<tr>
<th>Policy Contents</th>
<th>Effective Date: 03-01-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. POLICY STATEMENT</td>
<td></td>
</tr>
<tr>
<td>II. REASON FOR POLICY</td>
<td></td>
</tr>
<tr>
<td>III. SCOPE</td>
<td></td>
</tr>
<tr>
<td>IV. AUDIENCE</td>
<td></td>
</tr>
<tr>
<td>V. POLICY TEXT</td>
<td></td>
</tr>
<tr>
<td>VI. PROCEDURES</td>
<td></td>
</tr>
<tr>
<td>VII. RELATED INFORMATION</td>
<td></td>
</tr>
<tr>
<td>VIII. DEFINITIONS</td>
<td></td>
</tr>
<tr>
<td>IX. FREQUENTLY ASKED QUESTIONS</td>
<td></td>
</tr>
<tr>
<td>X. REVISION HISTORY</td>
<td></td>
</tr>
<tr>
<td>XI. COMPLIANCE</td>
<td></td>
</tr>
<tr>
<td>XII. POLICY EXCEPTION PROCESS</td>
<td></td>
</tr>
<tr>
<td>XIII. APPENDICIES</td>
<td></td>
</tr>
</tbody>
</table>

Effective Date: 03-01-2015  
Last Updated: 03-06-2015  
Responsible University Officer:  
Opinder Bawa  
Vice President, Chief Information Officer  
Policy Owner:  
Director, IT Infrastructure  
Policy Contact:  
ITS Help Desk
I. POLICY STATEMENT
   A. The university provides wireless communication services for faculty and staff in support of mission-related activities and to promote the cost-effective, appropriate and secure use of wireless devices.

II. REASON FOR POLICY
   A. The purpose of this policy is to preserve quality of service while supporting the university’s business objectives. Unauthorized modifications to the wireless network may lead to a change in service, quality and availability for everyone.

III. SCOPE
   A. The scope of this policy applies to all university wireless services. There is no provision for personal wireless service since such activity would severely impact all customers.

IV. AUDIENCE
   A. All parties are subject to the policy and standards set forth.
      1. All Employees, Faculty and Staff
      2. Residential students and guests living in university housing
      3. All contractors, vendors and any other 3rd parties entrusted with university job responsibilities.
      4. Campus Visitors using the "Visitors" wireless network.

V. POLICY TEXT
   A. Policy Statement
      1. The university wireless network is intended as a supplement to the wired network and for use with portable electronic devices; it is not intended to be a user’s sole connection to the university network or IT resources.
      2. The wireless network is not expected to provide the same quality of service as the university’s wired network infrastructure.
      3. When reliability and performance is critical, the university’s wired network infrastructure should be used.
      4. University computing resources, such as PCs, printers, servers and other critical IT equipment, must be connected to the wired network infrastructure.
5. Wireless networks and systems are subject to similar threats and vulnerabilities as data and voice networks. To reduce instances of expensive toll charges (fraud), denial of service attacks and damage to wireless equipment, users and supervisors should:
   a. Supervisors will submit an ITS Help Desk ticket to immediately deactivate USF accounts (which includes wireless access) for terminated and resigned personnel.
   b. Users shall not improperly access, move, modify or disrupt university-owned wireless equipment and service.
   c. Users shall not intercept wireless signals or transmissions.
   d. Access to wireless (and wired) switches and wiring closets shall be restricted to authorized individuals who require access to perform their job functions.
   e. Users will set a strong password for their USF accounts and change them according to the university password policy.
   f. Users shall not disclose (or write down) their wireless account password to anyone for any reason. REMEMBER: USF administrators don’t need your password to access accounts. Administrators can reset passwords.
   g. Users will not deploy personally-owned wireless access points.
   h. Users will contact ITS Help Desk within 30 days of arrival to the campus to register their personal wireless devices with Network Access Control (NAC).
   i. Users may only have three (3) personally-owned devices registered with the university NAC equipment at any time.

6. Temporary network wireless access may be granted to guests (visitors) who require access to the university on a regular or short-time basis.

7. Users may not extend university wireless coverage area.

8. Gaming is not permitted across the wireless network.

B. Standards

1. Those responsible for service, performance and modification to this policy must adhere to standards:
   a. Document existing and any modifications to the university wireless network
   b. Resolve & mitigate auditable events
      i. High risk events in 5 days
      ii. Medium risk events in 10 days
iii. Low risk events in 30 days
   c. Adhere to university wireless access point standards
   d. Where possible, increase wireless access coverage campus wide
   e. Provide a list of wireless devices that operate with existing access point equipment

C. **Auditable Events**
   1. For audit staff, the events and documentation below are needed to inspect the wireless network.
      a. Define acceptable wireless devices
      b. All wireless devices must login to network access control
      c. Wireless devices must meet minimum USF ITS Security

VI. **PROCEDURES**
   A. Below is a list of common set of procedures to increase the quality and services.

<table>
<thead>
<tr>
<th>Problem:</th>
<th>Action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to get wireless connection</td>
<td>Contact ITS and create a trouble ticket for a technician to initiate resolving the problem</td>
</tr>
<tr>
<td>Add a new wireless access point to the university network</td>
<td>Contact ITS and create a trouble ticket for a technician to initiate adding a new access point</td>
</tr>
<tr>
<td>Disable user wireless account</td>
<td>Contact ITS and create a trouble ticket for a technician to disable an existing wireless account</td>
</tr>
</tbody>
</table>

VII. **RELATED INFORMATION**
   A. For additional reference material related to this policy, please see:
      1. Information Security policy
      2. Password policy
      3. NAC standard operating procedure (SOP)
      4. Network Security policy
      5. Network Guest Access policy
VIII. DEFINITIONS
A. Gaming
   1. Entertainment game consoles, such as xBox P3, Nintendo, and Wii
B. Personally owned device
   1. A device not owned by the university, such as, electronic readers, smart phones and any other 802.11 compliant equipment.

IX. FREQUENTLY ASKED QUESTIONS
A. (None)

X. REVISION HISTORY
A. 12-09-2013 – First publication of policy
B. 03-01-2015 – Minor edits

XI. COMPLIANCE
A. Failure to follow this policy can result in disciplinary action in accordance with Human Resources Employment Handbook and Office of General Counsel employee and labor relations. In addition to temporarily or permanently being banned from use of the universities wireless network, disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS
A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of the VP of ITS.

XIII. APPENDICIES
A. (None)