Wireless Communication Policy

1. Overview
The purpose of this policy is to secure and protect the information assets owned by Duke University’s Fuqua School of Business (hereafter noted as “Fuqua”). Fuqua provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Fuqua grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Fuqua network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Infrastructure Team are approved for connectivity to a Fuqua network.

2. Scope
All faculty, employees, contractors, consultants, temporary and other workers (hereafter noted as “affiliates”) at Fuqua, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Fuqua must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Fuqua network or reside on a Fuqua site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular and smart phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

The Fuqua Infrastructure Team must approve exceptions to this policy in advance.

1 Policy Statement

1.1 General Network Access Requirements
All wireless infrastructure devices that reside at a Fuqua site and connect to a Fuqua network, or provide access to information classified as Fuqua Confidential, Fuqua Highly Confidential, or Fuqua Restricted must:

1.1.1 Abide by the standards specified in the Wireless Communication Standard.

1.1.2 Be installed, supported, and maintained by an approved support team.

1.1.3 Use Fuqua approved authentication protocols and infrastructure.

1.1.4 Use Fuqua approved encryption protocols.

1.1.5 Maintain a hardware address (MAC address) that can be registered and tracked.

1.1.6 Not interfere with wireless access deployments maintained by other support organizations.

1.2 Lab and Isolated Wireless Device Requirements
All lab wireless infrastructure devices that provide access to Fuqua Confidential, Fuqua Highly Confidential, or Fuqua Restricted information must adhere to section 1.1. Lab and isolated wireless devices that do not provide general network connectivity to the Fuqua network must:
1.2.1 Be isolated from the Fuqua network (that is it must not provide any corporate connectivity) and comply with the DMZ Security Policy or the Internal Security Policy.

1.2.2 Not interfere with wireless access deployments maintained by other support organizations.

1.3 Home Wireless Device Requirements

1.3.1 Wireless infrastructure devices that provide direct access to the Fuqua corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

1.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Fuqua corporate network. Access to the Fuqua corporate network through this device must use standard remote access authentication.

2 Enforcement

An affiliate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Fuqua.

3 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuqua network</td>
<td>A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to Fuqua services.</td>
</tr>
<tr>
<td>Fuqua connectivity</td>
<td>A connection that provides access to a Fuqua network.</td>
</tr>
</tbody>
</table>
| Information assets | Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
| MAC address        | The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network. |

4 Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Who made the revision</th>
<th>Change made</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-01-24</td>
<td>Fuqua Infrastructure</td>
<td>Initial issue.</td>
</tr>
</tbody>
</table>

This document was adapted from a draft created by the SANS Institute and is used by permission of the SANS Institute.