Wireless Communication Standard

1 Overview

The purpose of this standard 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 standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Fuqua network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Fuqua 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 standard. This standard 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 or 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.

3 Statement of Requirements

3.1 General Requirements

All wireless infrastructure devices that connect to a Fuqua network or provide access to Fuqua Confidential, Fuqua Highly Confidential, or Fuqua Restricted information must:

3.1.1 Use WPA2, Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.

3.1.2 Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES,, or CCMP) protocols with a minimum key length of 128 bits.

3.2 Lab and Isolated Wireless Device Requirements

3.2.1 Lab device Service Set Identifier (SSID) must be different from Fuqua production device SSID.

3.2.2 Broadcast of lab device SSID must be disabled.

3.3 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Fuqua network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

3.3.1 Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS

3.3.2 When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point

3.3.3 Disable broadcast of SSID

3.3.4 Change the default SSID name

3.3.5 Change the default login and password

4 References

In support of this standard, the following policies, guidelines, and resources are included:

- Information Sensitivity Policy
- Wireless Communication Policy

5 Enforcement

This standard is part of the Wireless Communication Policy and failure to conform to the standard is a violation of the policy. Any affiliate found to have violated the policy may be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Fuqua.

6 Definitions

Term	Definition
AES	Advanced Encryption System
Fuqua network	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Corporate connectivity	A connection that provides access to a Fuqua network.
EAP-FAST	Extensible Authentication Protocol-Fast Authentication via Secure Tunneling: authentication protocol for wireless networks.
EAP-TLS	Extensible Authentication Protocol-Translation Layer Security, used to create a secured connection for 802.1X by pre-installing a digital certificate on the client computer.
Enterprise Class Teleworker (ECT)	An end-to-end hardware VPN solution for teleworker access to the Fuqua network.
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.
PEAP	Protected Extensible Authentication Protocol, a protocol used for transmitting authentication data, including passwords, over 802.11 wireless networks
Service Set Identifier (SSID)	A set of characters that give a unique name to a wireless local area network.

TKIP	Temporal Key Integrity Protocol, an encryption key that's part of WPA.
WPA2	Wi-Fi Protected Access II
WPA-PSK	WiFi Protected Access pre-shared key

7 Revision History

Date	Who made the revision	Change made
2012-01-24	Fuqua Infrastructure	Initial issue

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