Smartlink Network Systems Ltd.	
Document Title	Wireless Communication Policy
Document Version	1.4
Document Approval Date	19th November 2010
Document Effective Date	31st December 2010
Document Last Updated Date	16th May 2012

Wireless Communication Policy

1 Overview

The purpose of this policy is to secure and protect the information assets owned by Smartlink. Smartlink provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Smartlink 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 technical requirements that wireless infrastructure devices must satisfy to connect to a Smartlink network. Only those wireless infrastructure devices that meet the requirements specified in this policy or are granted an exception by the IT Dept are approved for connectivity to a Smartlink network.

2 Scope

All employees, vendors, customers, contractors, consultants, temporary and other workers at Smartlink, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Smartlink must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Smartlink network or reside on a Smartlink site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, mobile/cellular phones and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting data. It is the responsibility of all Smartlink employees to follow these guidelines.

3 General Requirements

The wireless infrastructure device that allows wireless clients to connect to a Smartlink network must:

3.1 Use wireless key protection with minimum key length of 8 characters (64 bits).

3.2 Smartlink Employee wireless network should be hidden (non-broadcasted).

3.3 It is recommended to use different wireless networks (SSID) for Smartlink Guests.

3.4 Security recommended for Smartlink Employee wireless network to be WPA2-PSK & Smartlink Guests network to be WPA-PSK.

4 Lab and Isolated Wireless Device Requirements

In environments to conduct testing of wireless devices, the responsible testing teams should inform about their testing setups one day in advance to the IT Dept. A formal request for such testing needs to be submitted to IT dept by responsible testing teams. Configuration of the wireless devices being tested should be done in such a manner that there is no conflict in normal operations of Smartlink Wireless network- in consultation from IT Dept. It is the responsibility of all Smartlink employees to follow these guidelines.

4.1 Lab device Service Set Identifier (SSID) must be different from Smartlink production device SSID.

4.2 Lab device wireless Channel must be different that the existing-site-wireless-channel of Smartlink production device.

5 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Smartlink network, such as those behind remote hardware VPN, are recommended to:

5.1 Enable Wireless Key Security.

5.2 Change the default SSID wireless name.

5.3 Change the default login and password.

Employees using home wireless setups to connect to Smartlink networks must notify IT dept & follow above recommendations.

6 Remote Sites / Branches Wireless Device Requirements

The wireless infrastructure device setup at branches/remote locations requires branch employees to pre-notify IT Dept for implementing standard wireless setup. All Remote Sites / Branches wireless infrastructure devices that provide access to a Smartlink network (such as those behind remote hardware VPN) require:

6.1 Remote site (branch) wireless networks (where no IT support staff is available) are recommended to comply with section-3 of this document.

6.2 Users/ Employees in these sites / branches maintaining wireless infrastructure should approach IT Dept for standardized wireless network deployments.

6.3 Further to these deployments, wireless device passwords will not be disclosed to site employees for security reasons. In case of any issues, IT Dept will provision remote support to such locations in co-ordination with site employees.

7 Enforcement

Employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any violation of this policy by a temporary worker, contractor or vendor/customer may result in the termination of their contract or assignment with Smartlink.

8 Definitions

Term	Definition
Smartlink network	A wired or wireless network including indoor and outdoor networks that provide connectivity to corporate services.
Corporate connectivity	A connection that provides access to a Smartlink network.
Hardware VPN	An end-to-end hardware VPN solution for remote access to the Smartlink 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.
Service Set Identifier (SSID)	A set of characters that gives a unique name to a wireless local area network.
Wireless Security Key	PSK (Pre-Shared Key) Security Key of wireless networks.
WPA-PSK	WiFi Protected Access pre-shared key
WPA2-PSK	Revision 2 of WiFi Protected Access pre-shared key

9 Revision History

Version	Date	Author	Remarks
1.0	24 th September 2009	Kiran Gole	Document created
1.0	15 th October 2009	Sandeep S	Discussed with Security Committee / Head
1.1	15 th October 2009	Kiran Gole	Document updated.
1.1	15 th October 2009	Sandeep S	Approved by Security Committee / Head
1.2	13th November 2009	Kiran Gole	Document updated.
1.2	13th November 2009	Sandeep S	Approved by Security Committee / Head
1.3	8 th November 2010	Kiran Gole	Document updated.
1.3	19 th November 2010	Shridhar K	Approved by Security Committee / CTO
1.4	16th May 2012	Mayur Gujar	Name & Logo updated.