**Wireless Communication**

**Policy**

Prepared By

**IT Security**

**VERSION: 1.0**

All rights reserved. This document is a proprietary product of IT Security and, as such, any unauthorized use, disclosure, or reproduction of this publication or portions thereof in any form, without written permission from IT Security, is strictly prohibited. Any printed copy of this document is uncontrolled

**CHANGE HISTORY**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** | **Pages affected** | **Remark** |
| 1.0 |  |  |  |  |  |

Table of Contents

**PURPOSE 4**

**SCOPE 4**

## POLICY 4

***WIRELESS PLANNING STAGE 4***

***ACCESS POINT CONFIGURATION 4***

***CLIENT SYSTEM CONFIGURATION 5***

***APPROVED TECHNOLOGY 5***

***ENCRYPTION AND AUTHENTICATION 5***

**ENFORCEMENT 6**

**PURPOSE**

This policy prohibits access to Organization networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by I. T. Security are approved for connectivity to Organization's networks or within the Organization environment.

1. **SCOPE**

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) within Organization’s environment. This includes any form of wireless communication device capable of transmitting packet data.

1. **POLICY**
   1. **Register Access Points and Cards**
      1. All wireless Access Points / Base Stations within Organization environment must be registered and approved by I. T. Security. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the party maintaining thewireless system. I. T. Security reserves the right to view for this register whenever required.
      2. Request for a wireless connection must be duly authorised by the requestor’s Unit Manager and IT Security Department. The following information should be stated in the request:
         1. Purpose of the request
         2. Information to be transmitted
         3. Duration or period of the request
2. ***Wireless Planning Stage***

*In planning, below are the considerations from security point of view:-*

* + - 1. *Access point architecture (i.e. Centralization/decentralize access point)*
      2. *Fat/thin client*
      3. *Area of coverage*
      4. *Implementation of wireless IDS*
      5. *Requirement for account*

1. ***Access Point Configuration*** 
   * + 1. *Turn off service set identifier (SSID) broadcast on all internal, non-public, non-guest access points.*
       2. *Change SSIDs on all internal, non-public, non-guest access points to unique names, and consider not using names that reveal locations or owner.*
       3. *Limit coverage of access points to areas that need them the most, and minimize coverage in unwanted areas via careful placement access points and by limiting transmission strength (by antenna setting and transmitter output setting).*
       4. *Whenever technology permits, migrate to the latest WLAN network interface cards (NICs), wireless drivers, supplicants, and access points on all new purchases.*
       5. *Avoid the use of pre-shared keys (PSKs) in WPA or WPA2. WPA and WPA2 for Enterprise mode are recommended, for better authentication mechanism.*
       6. *If public or guest access is to be allowed, use virtual LAN (VLAN) tunnels to route users to a point outside the firewall.*
2. ***Client System Configuration***
   * + 1. *Every laptop with a wireless NIC must have a personal firewall installed. At minimal, use operating system default firewall (i.e. Windows XP Firewall).*
       2. *Keep WLAN card drivers and system patches up to date.*
       3. *Turn off peer-to-peer/ad hoc networking.*
       4. *Only one WLAN connection manager allowed to be active on a client system.*
       5. *Wireless and wired NICs should not be allowed to be active at the same time on a client system. Isolated approach recommended.*
       6. *Shut down split tunnels on VPNs or adjust personal firewalls to prevent exposure of client ports.*
3. **Approved Technology**

All wireless LAN access must use corporate-approved vendor products and security configurations endorsed by I.T. Security.

1. **Encryption And Authentication**

All connections for the wireless network must comply with at least 2 of the following requirements:-

* + - 1. Wireless implementations must maintain point to point encryption of strong cipher strength. Encryption standards must comply with Organization’s Acceptable Encryption Guideline.
      2. All implementations must be able to filter unauthorised MAC address.
      3. *Anticipate the need to support more than one type of authentication and airlink security combination.*

1. **ENFORCEMENT**

# All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any Organization staffs who fail to comply with the Organization’s security policies, or circumvent/violate any security systems and/or protection mechanisms.

# Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.

* 1. Organization’s staff must ensure that Organization’s contractors and others parties authorized by the Organization using its internal computer systems, comply with this policy.
  2. Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.