

## 3.9 Wireless LAN Policy

**A visitor was caught connecting to the office wireless network while sitting in his/her car in the car park. Investigation revealed that the office's confidential data has been compromised.**

**Audience** All User

**Policy** All Wireless LAN must be secured to protect against unauthorized access, modification, disclosure, interruption or destruction of information assets.

**Standard** Security features including but not limited to authentication, encryption, MAC address filtering must be enabled. In addition, surveillance system must be deployed to monitor and detect alien traffic.

### **Procedure**

(1) Wireless LAN deployment must have authorization from the CIO of the organization and written permission from the State CSO.

(2) Wireless LAN administrator is to design a secure infrastructure as follows:

- (i) Wireless LAN must be on a different segment from wired LAN.
- (ii) Surveillance system must be incorporated to detect unauthorized traffics.
- (iii) Wireless Access Point signal strength must only limited to the designated area.

- (iv) Access point must be installed at a secure location to prevent from being tampered.
- (3) Wireless Access Point must be secured with at least the following configurations:
- (i) Latest Encryption standard must be used.
  - (ii) MAC address filtering must be **enabled**.
  - (iii) SSID Broadcast must be **disabled**.
  - (iv) Can only use **static IP** address unless otherwise determined by the organization.
  - (v) All users devices must be configured by network administrator before connecting to wireless access point.
  - (vi) Access control must be implemented with user authentication

Refer to the 3.8.1 Password Policy in sgCert ([www.sgcert.org](http://www.sgcert.org)).

## **Guidelines**

- (1) Wireless LAN can be implemented only when wired LAN is not feasible OR only at designated area for visitor access.
- (2) Designated area means certified safe area for wireless access.
- (3) Network Administrator is a technical personnel that is appointed by the CIO of the organization.
- (4) Visitor means invited guest.
- (5) Secure location means hidden location.