



**Islamic Republic Of Afghanistan  
Kabul Municipality**



# **WIRELESS NETWORKING SECURITY POLICY**

H.E Mohammad Yonus Nawandesh

Mayor Signature: \_\_\_\_\_



# Islamic Republic Of Afghanistan Kabul Municipality



## Purpose

The purpose of the Kabul Municipality (KM) Wireless Network Security Policy is to define the security requirements necessary to ensure the confidentiality, integrity and availability of all wireless communications that are used to transmit sensitive information.

## The Policy

Wireless devices or networks used to access, store, process, or transmit Kabul Municipality's information or access internet must be implemented in a secure manner.

Wireless devices and networks enable un-tethered communications to mobile users. Improperly installed, configured or managed wireless technology presents a significant risk to the confidentiality of information. Wireless network security refers to the protection of wireless network hardware, software, and the information contained in them from threats caused by the inherent vulnerabilities in the technology and its implementation.

## Scope

This policy applies to all wireless devices, networks, services, and technologies used to access, store, process or transmit KM information or connect to internet. The term "wireless" refers to any technology that does not use cables.

**Wireless** includes radio frequency (i.e. satellite, microwave, radio) and optical (i.e. infrared) technologies.

**Wireless networks** include both wireless local area networks (WLANs) and wireless wide area networks(WWAN).

**Wireless devices** are any end-user device that uses wireless technology to communicate. These include but are not limited to: cellular phones, laptop computers, desktop computers with wireless NIC and printers.

**Wireless Access Points/ Routers** are wireless transceivers used in KM network. They are typically used to provide wireless connectivity.

## Appropriate Use

- Wireless devices may not be used to gain or attempt to gain unauthorized access to any network. This includes accessing KM network and the internet where the user has not been granted access.
- Only approved services and applications may be used with wireless devices.
- Any planned wireless connection(s) must be reviewed and approved in advance of installation by the KM IT Department.



# Islamic Republic Of Afghanistan Kabul Municipality



## Access Control

- Access to the KM's networking and computing infrastructure via a wireless connection is considered remote access and must utilize strong authentication and encryption.
- Appropriate encryption must be used.

## Risk Assessment

The KM IT Department should employ security measures commensurate with the risk associated with the wireless network. If the network is used for transmission of KM's sensitive material, proper encryption should be applied to the material.

- Due to the ever changing threats and vulnerabilities, risk assessments should be conducted on a periodic basis no less than annually to provide an accurate picture of the total risk to Kabul Municipality.
- A risk assessment should be performed to ensure the capabilities of protection for the technologies utilized. A risk assessment should include but not be limited to; identifying data sensitivity, network vulnerabilities, and critical services. The focus should be to identify potential threats and vulnerabilities.

## Implementation

Wireless networks enable computers to be interconnected using standard network protocols such as IP. Wireless networking technology relies on radio frequencies and data transmission. The most widely used wireless standard is the Institute of Electrical and Electronic Engineers (IEEE) 802.11 which has been adopted by the Office of Information Technology Services (ITS) to serve as the state-wide standard.

### Modes of Operation

Two (2) types of wireless networks are possible, and they differ on how wireless devices communicate with each other. Wireless LANs (WLANs) operate in either the ad-hoc or the infrastructure mode.

- Ad-hoc networks have multiple wireless clients communicating with each other as wireless peers to share data among themselves without the aid of a wireless access point (AP). This mode is also known as independent basic service set (IBSS).
- An infrastructure WLAN consists of several clients communicating with an access point which is usually connected to a wired network like a LAN. Most WLANs operate in infrastructure mode because they require access to the wired LAN to use services such as printers and file servers. This mode is also known as the basic service set (BSS).

## Authentication

All users of WLANs are required to authenticate before being allowed to access the network.