



الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

## AASTMT Wireless Network Usage

<b>Classification</b>	Information Security
<b>Version</b>	1.0
<b>Status</b>	Not Active
<b>Prepared Department</b>	Computer Networks and Data Center
<b>Approved Authority</b>	AASTMT Presidency
<b>Release Date</b>	19/4/2015
<b>Effective Date</b>	19/4/2015

### Overview

Wireless networking is an extension of the AASTMT existing wired network infrastructure. It allows users with wireless enabled infrastructure devices to access university network resources and the public Internet. The AASTMT provides multiple levels of wireless access services that offer either unencrypted or encrypted over-the-air security.

### Purpose

The purpose of this policy is to ensure the proper use of AASTMT wireless network and specifies the conditions that wireless infrastructure devices must satisfy to connect to AASTMT wireless network. Only those wireless infrastructure devices that meet the standards specified in this policy are approved for connectivity to AASTMT wireless network. AASTMT reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

### Scope

This policy covers everyone who works for or grants access to AASTMT for the appropriate use of AASTMT wireless network using all wireless infrastructure devices, laptops, cellular phones, and personal digital assistants (PDAs).



الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري  
Arab Academy for Science, Technology & Maritime Transport

## Policy

- ✓ All wireless devices connected to AASTMT wireless networks must use the most up-to-date anti-virus software and up-to-date operating system security patches.
- ✓ Users of wireless devices that are not AASTMT owned equipment must configure the equipment to comply with this wireless security policy and other and Network security policies.
- ✓ All persons approved to connect their wireless devices to AASTMT network may be subject to restricted network resource access per their specified business requirements.
- ✓ Wireless gateways will be set up and managed by AASTMT network and security admins with ease, fast, secure and protected Authentication protocol.
- ✓ All wireless devices connected to AASTMT network must be registered and approved by AASTMT policy. All wireless devices are subject to periodic monitor, tests and audits.
- ✓ All wireless LAN hardware implementations shall utilize Wi-Fi certified devices that are configured to use the latest security features available.
- ✓ It is prohibited to add any wireless access point or wireless gateway without permission form computer network and data center.

## Monitoring

For your safety and the safety of AASTMT network and information, all data packets that passes through the wireless network is automatically scanned and monitored by administrative privileges and by many levels. AASTMT has the capability and reserves the right to access, review, and copy or delete any data for any purpose. AASTMT may monitor wireless transferred data without prior notice. AASTMT is not obliged to monitor these data.

## Enforcement

Beyond this security policy you should make sure you have a solid understanding of other AASTMT security policies and roles. Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

### Revision History

Null.

### Related Policies

- ✓ AASTMT Acceptable Use Policy.
- ✓ AASTMT Email Use Policy.
- ✓ AASTMT Internet Use Policy.
- ✓ AASTMT User ID and Password Policy.
- ✓ AASTMT VPN Policy.