UTHM WIRELESS GUIDELINE

1) OBJECTIVE

The objective of this guideline is to prohibit the access to UTHM networks via unsecured wireless communication mechanisms. Only the wireless system that meets the criteria of this guideline or that has been granted an exclusive waiver by the Director of PTM is approved for connectivity to UTHM network.

2) SCOPE

This guideline covers all wireless data communication devices which are connected to any of UTHM's internal networks or that are residing on UTHM property. This guideline also applies to any form of wireless communication device capable of transmitting packet data.
Previously existing connections should not be an exception, unless a waiver explaining why compliance is not met and outlining a migration plan which is approved by the Director of PTM.

3) GUIDELINE STATEMENT

The guideline statements are as follows;

1. Devices connected to the UTHM network must adhere to current UTHM ICT standards. These standards are subject to change on short notice, or without notice if a security threat arises.

2. PTM maintains an official wireless network distributed over the entire campus. The official wireless network is configured with a user authentication system which is suitable for the UTHM community use. This is the only network that is approved to offer wireless services to the UTHM community. Any wireless devices found to interfere with this network will be disconnected.

3. All Wireless Access Points / Base Stations that are used must be registered and approved by PTM. These Wireless Access Points / Base Stations are subject to periodic penetration tests and audits.

4. Vendor products and security configurations of all wireless local area network access must be approved by PTM.

5. All wireless local area network must be configured to drop all unauthenticated and unencrypted traffic. Wireless implementations must maintain point to point hardware encryption compliant to current standards. All implementations must support a hardware address that can be registered and tracked. All implementations must support and employ a strong user authentication which checks against an external database.

6. When possible, the SSID should not broadcast the name to reduce possible unauthorized connections.

7. When a wireless network is connected to the UTHM network, the connected machines are also subject to the same rules and regulations that apply to UTHM-owned equipment.

4) RESPONSIBLITY FOR IMPLEMENTATION

The responsibility for the implementation of this guideline is with the Head of Department, Network Department, PTM.

5) ENTITIES AFFECTED BY THIS GUIDELINE

Any of UTHM staff, students, consultants, contractors, vendors and others who install, manage and use networking facilities.