Wireless Network Infrastructure Set Up Policy at METU Campus Network

1. Purpose

This document is prepared in order to designate the principles to abide for those units (academic and administrative corporate bodies) and natural persons who set up wireless access devices with the purpose of connecting to the METU campus domain network.

2. Acronyms and Definitions

CC: The Computer Center.

IP address: *"Internet Protocol"* address. The IP address formatted as 144.122.xxx.xxx which is assigned for every computer that is used for communication and connected to the METU campus domain network.

MAC address: *"Media Access Control"* address. The unique identification information set by the manufacturer on the network access card of any computer.

Security Threats: The various methods (viruses, Trojan horses etc.) that spread wide and provide illegal access to personal / corporate information making use of the security breaches of the computers connected to the network and thus threaten security of information and network access.

Data Traffic: The data conveyed on the network.

SSID: This is the acronym for *"**S**ervice **S**et **ID**entifier"* which means the identity of the service provider. It defines the name of the wireless network.

3. The Scope

This document covers information and the principles related to the installation and the maintenance of the network security for pieces of equipment, which can be interpreted as wireless devices, in order to connect to the campus area network of METU. In order to maintain the campus network properly and to provide security of the corporate / personal information on the computers connected to the network it is imperative that the installation and settings be performed in correlation with the instructions given on this document. The units are obliged to comply with the principles stated on the METU Information Technology Resources Use Policy Document (http://computing-ethics.metu.edu.tr).

4. The Policy

1. The regulations of wireless network broadcast in METU campus area is governed by the METU CC.
2. Prior to the decision of installing a wireless access device, the facilities provided by the CC should be evaluated (http://www.bidb.odtu.edu.tr), and the services given by the CC should be preferred to be used primarily.
3. Access to the METU campus area network via wireless network access devices installed by units and persons may only be provided to users designated in the METU Information Technology Resources Use Policy Document (http://computing-ethics.metu.edu.tr). Access authorization should not be provided to any corporate body or natural persons other than the ones stated in that document.
4. Units and persons are obliged to bear the technical and the administrative responsibilities for the wireless network service that they provide.
5. The liability of any dispute that may arise from the conveyed data traffic over the wireless network access device installed by the units and persons is to the unit or person providing the service.
6. The units and the persons are responsible for taking the necessary measures to provide the security of the software running on the wireless network access device.
7. The units and the persons can only run their wireless network access devices **only on the 13th channel**. The other channels are assigned for the wireless network services that the CC provides within the campus. In cases where using channels other than the 13th channel is deemed necessary, one or more of the other channels may temporarily be made available to the users, when the related unit or the person applies to the CC in writing.
8. The units and the persons should operate their wireless network access devices at low output power levels so as not to cause interference with the other wireless broadcast in the vicinity and cause broadcast disturbances.

5. General Principles

For the information technology services provided via **the wireless network the units and the persons are responsible (the one they have installed)**, they are obliged to comply with the principals stated below:

1. **The default Administrator Password for the device must be changed:** For the sake of security the default administrator password used for managing the network must be changed to a combination different from the default password.
2. **Unused services must be shut down:** The services (web, telnet, etc.) not functioning any longer should be shut down due to reasons of probable breach of security.
3. **User authorization methods should be set:** For cases where access to METU campus network via the wireless network access device is provided authorization mechanisms (access passwords, MAC based access, certificate access etc.) are to be set and put into function.
4. **No way, should unauthorized access be permitted:** The right to make use of the wireless network access device in order to connect to the campus network of METU should be provided to the authorized users alone and should not be made available to any client who receives the broadcast.
5. **Data Encryption methods should be put into practice:** While accessing the campus network of METU via the wireless network access device the data traffic between the computer and the wireless network access device should flow encrypted (This is accomplished by WEP and WPA for wireless network structures. The CC recommends the use of WPA).
6. **The default SSID should be changed:** In order to prevent trial and error attacks aimed at the wireless network device the default value of the SSID should be changed.
7. **The devices of the personal users should not do SSID broadcast:** Endangering the security of the wireless network device and the computers that connect to the campus network of METU via that device should be prevented.
8. **The broadcast of the wireless network device should not reach outside the building:** The wireless network access device should be mounted at the centre of the building so as to maintain broadcast to a minimum outside the building so that it does not cause interference

with the neighboring broadcasts and cause deterioration of the transmission.

9. **The software updates of the wireless network access device should be performed**: The updates of the software used in the wireless network access device should be made periodically in order to provide measures to prevent against probable security breaches.
10. **The installation manuals should be read:** Before the installation, all the manuals that come along with the device should be read and the installation be carried out in accordance with these manuals.

6. Implementation and Sanctions

The units and persons are obliged to comply with the principles implied with this document during the installation of the wireless network access device. In case of failure in complying with these principles, depending on the prevailing conditions, the CC keeps the right to apply the necessary sanctions, from notifying the responsible persons to temporary or permanent inhibition of access to the service, in order for the campus network to function properly.